LDAP 相关介绍、在话机上的使用及不同系统下服务器搭建

版本：<1.1>

发布日期：<2018-5-24>

目录

1 介绍

1.1 概述

LDAP 是 Lightweight Directory Access Protocol（轻量级目录访问协议）的缩写。特指基于 X.500 的目录访问协议的简化版，运行在 TCP/IP 或者其他的面向连接的传输服务之上。LDAP 以信息目录的形式存在，在该目录中可以只定义一次用户和组，而在多台机器和多个应用程序间共享它们。

LDAP 定义与目录服务进行通信所使用的操作，如何找到目录中的实体，如何描述实体属性，以及许多安全特性。这些安全特性可用于对目录进行身份验证，控制对目录中实体的访问。目录服务是一种特殊的数据库系统，其专门针对读取、浏览和搜索操作进行了特定的优化。目录一般用来包含描述性的，基于属性的信息并支持精细复杂的过滤能力。目录一般不支持通用数据库针对大量更新操作需要的复杂的事务管理，而目录服务的更新则一般都非常简单。这种目录可以存储文本资料、二进制图片等信息，例如联系人列表、个人信息、web 链接、jpeg 图像等。为了访问存储在目录中的信息，就需要使用运行在 TCP/IP 之上的访问协议—LDAP。如图 1-1-1

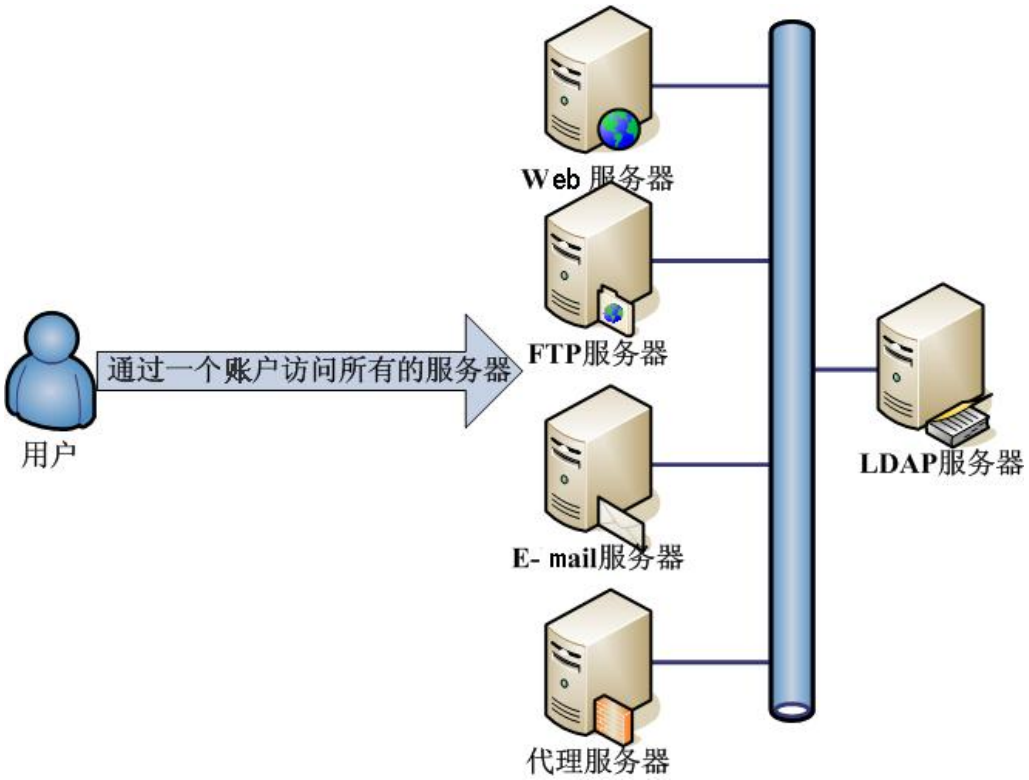

图 1-1-1

1.2 LDAP 信息模型

LDAP 目录中的信息是按照树型结构组织，具体信息存储在条目(entry)的数据结构中。条目相当于关系数据库中表的记录，条目是具有区别名 DN（Distinguished Name）的属性（Attribute），DN 是用来引用条目的，DN 相当于关系数据库表中的关键字。属性由类型（Type）和一个或多个值（Values）组成，为了方便检索的需要，LDAP 中的 Type 可以有多个 Value。LDAP 以树型结构存储的信息，在树根一般定义国家(c=CN)或域名(dc=com)，其下往往定义一个或多个组织(organization)或组织单元(organizational units)。LDAP 系统结构图如图 1-2-1。

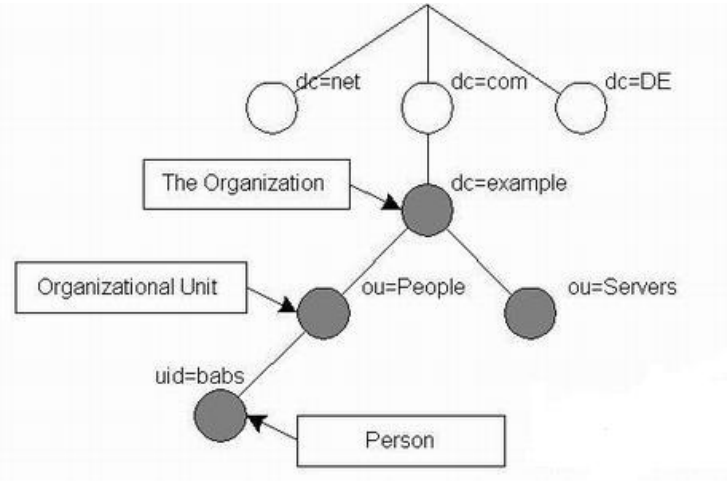

图 1-2-1

如图 1-2-2 的例子中，树的根结点是一个组织的域名（dlw.com），其下分为 3 个部分，分别是 managers、people 和 group，可将这 3 个组看作组织中的 3 个部门，如 managers 用来管理所有管理人员，people 用来管理登录系统的用户，group 用来管理系统中的用户组。当然，在该图中还可继续增加其他分支。

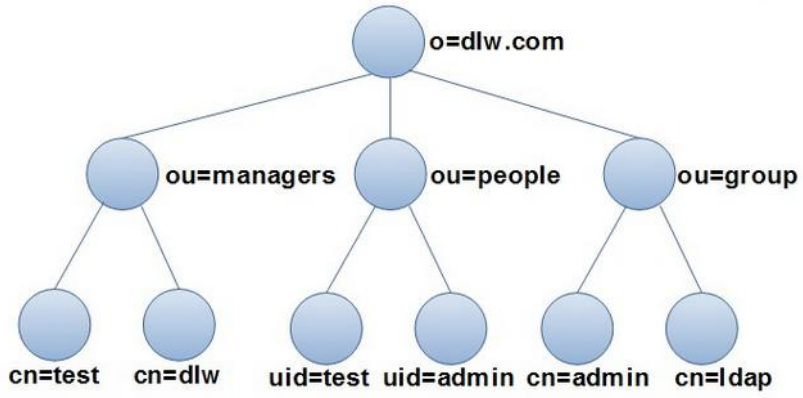

图 1-2-2

1.3 LDAP 中的 objectClass 与 Attribute

LDAP 支持对条目设定可选和必选的属性，这是由一个特殊的称为对象类别(objectClass)的属性来实现的。该属性的值决定了该条目必须遵循的一些规则，其规定了该条目能够及至少应该包含哪些属性。

LDAP 中，一个条目必须包含一个 objectClass 属性，且需要赋予至少一个值。每一个值将用作一条 LDAP 条目进行数据存储的模板；模板中包含了一个条目必须被赋值的属性和可选的属性。

objectClass 有着严格的等级之分，最顶层是 top 和 alias。例如，organizationalPerson 这个 objectClass 就隶属于 person，而 person 又隶属于 top。

objectClass 可分为以下 3 类：

- 结构型（Structural）：如 person 和 organizationUnit；
- 辅助型（Auxiliary）：如 extensibeObject；
- 抽象型（Abstract）：如 top，抽象型的 objectClass 不能直接使用。

下面列出部分常用 objectClass 要求必设的属性。

- account：userid。
- organization：o。
- dcobject：dc。
- person：cn 和 sn。
- organizationalPerson：与 person 相同。
- organizationalRole：cn。
- organizationUnit：ou。
- posixGroup：cn、gidNumber。
- posixAccount：cn、gidNumber、homeDirectory、uid、uidNumber。

属性（Attribute）类似于程序设计中的变量，可以被赋值。常见的 Attribute 含义如下：

- c：国家。
- dc：domain Component，常用来指一个域名的一部分。
- givenName：指一个人的名字，不能用来指姓。
- l：指一个地名，如一个城市或者其他地理区域的名字。
- mail：电子信箱地址。
- o：organizationName，指一个组织的名字。
- ou：organizationalUnitName，指一个组织单元的名字。
- cn：common name，指一个对象的名字。如果指人，需要使用其全名。
- sn：surname，指一个人的姓。

- telephoneNumber：电话号码，应该带有所在的国家的代码。
- uid：userid，通常指某个用户的登录名

注：objectClass 是一种特殊的 Attribute，它包含其他用到的 Attribute 以及其自身。

1.4 适用型号

- X3S/X4/X5S/X6/X7/X7C/X210/X210i/X3U/X4U/X5U/X6U
- F3/F4

1.5 目标受众

此文档针对需要测试 LDAP 应用的内部人员和客户。

1.6 术语表

关键字	英文全称	含义
C	Country	国家，如“CN”或“US”等。
DC	Domain Component	域名，其格式是将完整的域名分成几部分，如域名为 winline.com 变成 dc= winline,dc=com
O	Organization	组织名，如“winline”
OU	Organization Unit	组织单位，类似于 Linux 文件系统中的子目录，它是一个容器对象，组织单位可以包含其他各种对象（包括其他组织单元），如“test”
UID	User Id	用户 ID，如“tom”
CN	Common Name	公共名称，如“Thomas Johansson”
SN	Surname	姓，如“Johansson”
DN	Distinguished Name	惟一辨别名，类似于 Linux 文件系统中的绝对路径，每个对象都有一个惟一的名称，如“uid=tom,ou=test,dc= winline,dc=com”
RDN	Relative dn	相对辨别名，类似于文件系统中的相对路径，它是与目录树结构无关的部分，如“uid=tom”或“cn=Thomas Johansson”

2 在 windows 搭建 openLdap

2.1 openLDAP 下载及安装

2.1.1 下载

本小节主要讲解在 win10 企业版环境下下载，安装 OpenLdap 。Windows 的 OpenLdap 是免费软件，可以在下面的链接中免费获得：
http://www.userbooster.de/en/download/openldap-for-windows.aspx?l=en

2.1.2 安装

1. 点击下载好的 exe 文件，会弹出下面的选择框，选择 Yes. 如图 2-1-1

图 2-1-1

2. 一直点击 next，使用它默认的配置。如图 2-1-2

图 2-1.2

3. 一直到路径选择框，将其改为自己想要下载的路径。如：D:\OpenLdap。如图

2-1-3

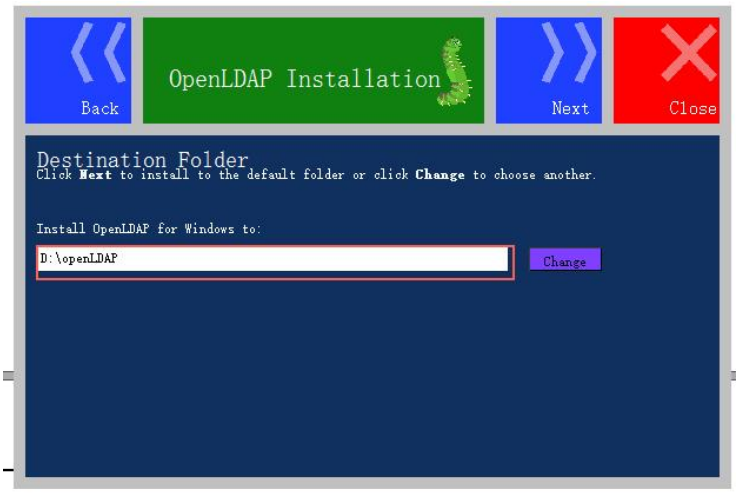

图 2-1-3

4.在弹出安装界面时，点击 install 按钮开始安装。安装成功后点击 close 按钮关闭。

如果在安装中有任何问题，可以点击下面的链接寻找安装中出现问题的解决方法：

http://www.userbooster.de/en/support/feature-articles/openldap-for-windows-installation.aspx

如果提示缺少 gssapi32.dll 或 gssapi64.dll，可以在网上下载后放到 openLdap 的安装路径中。

2.2 配置 openLDAP Server

2.2.1 修改 slapd.conf 文件

在 openLDAP 的安装目录下，修改 slapd.conf 文件，在 slapd.conf 的文件中查找相应的配置：如图 2-2-1

Suffix “dc = maxcrc, dc = com”

Rootdn “cn = Manager,dc = maxcrc, dc = com”

```
database    mdb
suffix      "dc=maxcrc,dc=com"
rootdn      "cn=Manager,dc=maxcrc,dc=com"
# Cleartext passwords, especially for the rootdn, should
# be avoid.  See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
rootpw    {SSHA}G8nIcSW6gSCQ6bKD8eCb4M0dJ/olUDDe
```

图 2-2-1

其中，Suffix 是用来定义域名的组件。Rootdn 是用来定义管理用户。

我们也可以将域名改变为 fanvil.com 或是其他的域名，其中管理员的域名也要更改

例如：如图 2-2-2

```
Suffix    “dc =fanvil, dc = com”
Rootdn    “cn = Manager, dc =fanvil, dc = com”
```

```
database    mdb
suffix      "dc=fanvil,dc=com"
rootdn      "cn=Manager,dc=fanvil,dc=com"
# Cleartext passwords, especially for the rootdn, should
# be avoid.  See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
rootpw    {SSHA}G8nIcSW6gSCQ6bKD8eCb4M0dJ/olUDDe
```

图 2-2-2

如果域名中包含其他的组件，那么就像下面这样：如图 2-2-3

```
Suffix    “dc =fanvil, dc = com, dc = cn”
Rootdn    “cn = Manager, dc =fanvil, dc = com,dc = cn”
```

```
database    mdb
suffix      "dc=fanvil,dc=com,dc=cn"
rootdn      "cn=Manager,dc=fanvil,dc=com,dc=cn"
# Cleartext passwords, especially for the rootdn, should
# be avoid.  See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
rootpw    {SSHA}G8nIcSW6gSCQ6bKD8eCb4M0dJ/olUDDe
```

图 2-2-3

2.2.2 修改密码

1. 先将 ladp 服务关闭
2. 点击 开始 - 运行。
3. 输入 cmd，进入命令行界面。（如果 window10 没有找到运行，可以直接输入 win + r 后输入 cmd）
4. 切换到安装目录，执行 slappasswd，输入两遍新密码以确保输入无误。
5. 得到一个暗码，将暗码放到 slapd.conf 中。如图 2-2-4 和 2-2-5
6. 重新启动服务。

注：如果您的 cmd 无法进行复制操作可以将 slappasswd 命令生成的暗码重定向到一个其他文件中或使用快捷键 Ctrl +M 进行选择后按 Ctrl +C 进行复制操作。

```
# slappasswd > \home\test.txt
 //将 slappasswd 命令生成的暗码放到 home 目录下的 test.txt 文件中
```

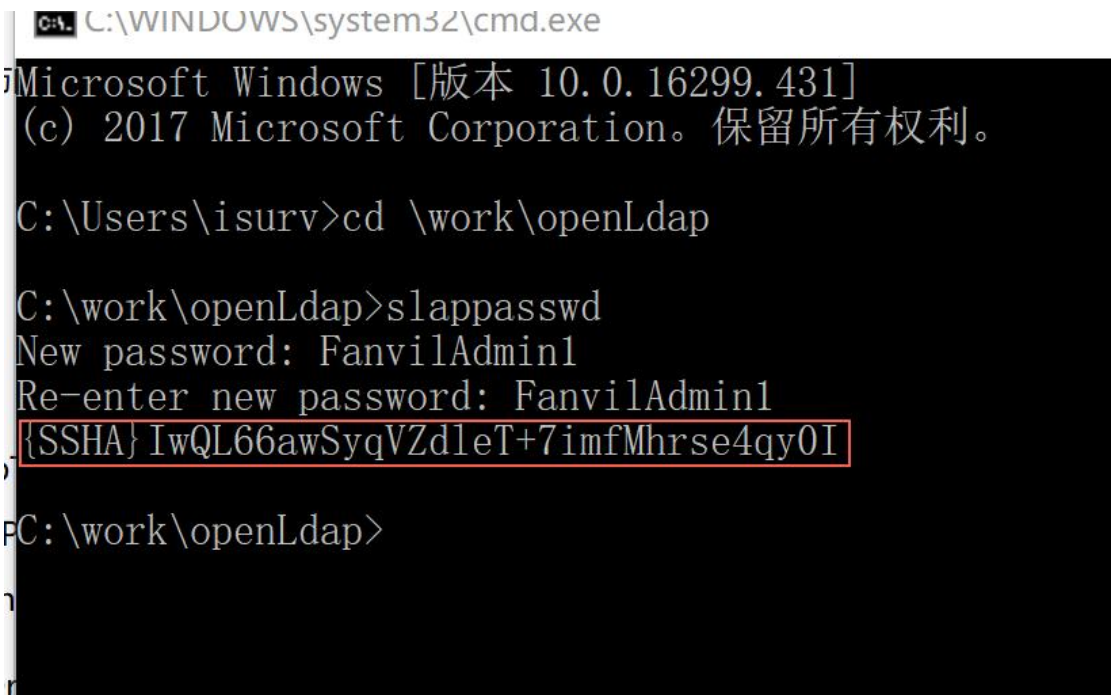

图 2-2-4

```
database    mdb
suffix      "dc=fanvil,dc=com"
rootdn      "cn=Manager,dc=fanvil,dc=com"
# Cleartext passwords, especially for the rootdn, should
# be avoid.  See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
rootpw    {SSHA}IwQL66awSyqVZdleT+7imfMhrse4qy0I
```

图 2-2-5

2.3 启动 Slapd 服务

2.3.1 启动 Slapd 流程

方法 1：

1. 点击 开始 - 运行。

2. 输入 cmd，进入命令行界面。（如果用户使用的是 window10 系统，没有找到运行，可以直接输入 win + r 后输入 cmd）

3. 进入对应的 LDAP 安装的路径，例如路径是 C:/办公软件/LDAP，（如果条件允许，建议不安装在 C 盘中，且路径为纯英文）并输入执行命令：slapd.exe -d 1 -f ./slapd.conf

如图 2-3-1

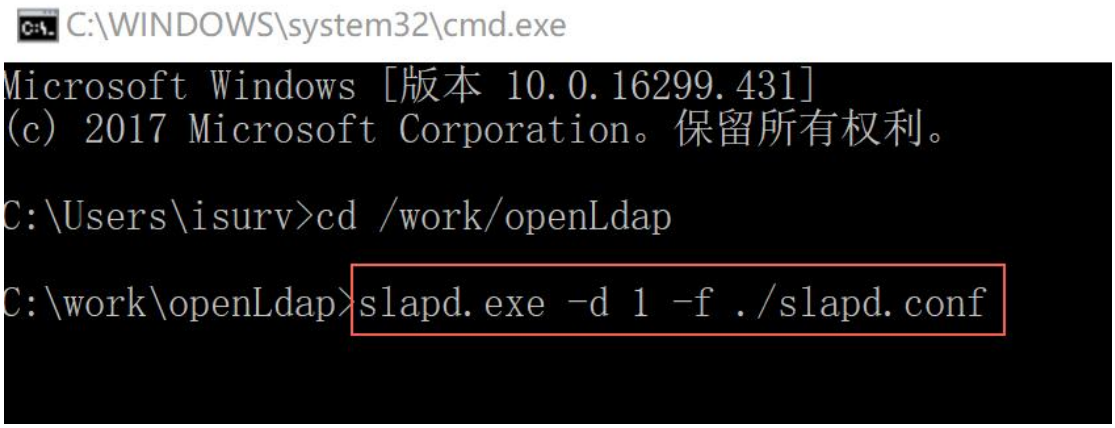

图 2-3-1

4.成功后会看到下图中红框中的字段：slapd starting.如图 2-3-2

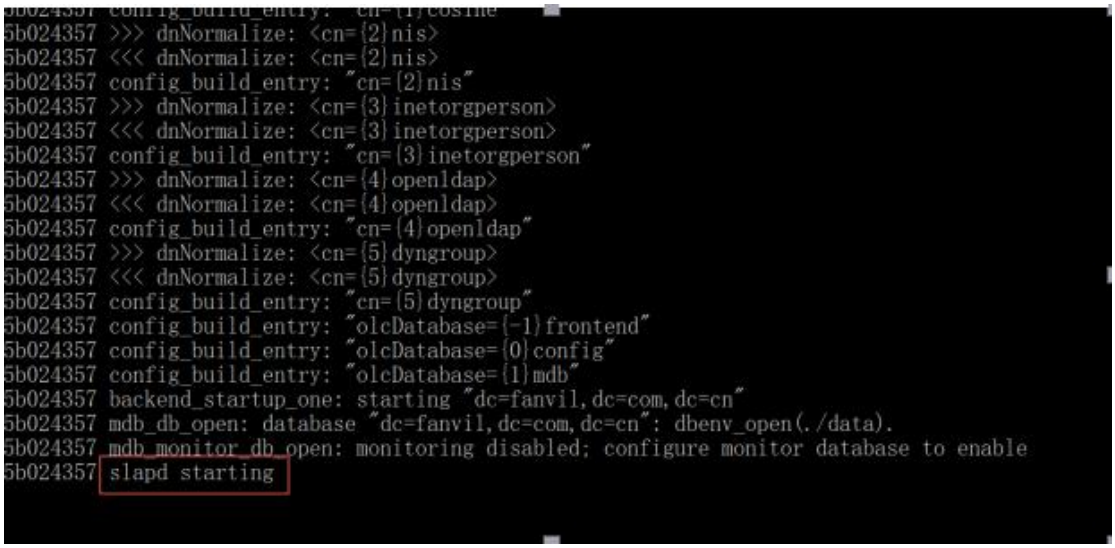

图 2-3-2

注意：不要关闭 cmd 窗口，以确保 LDAP 服务器继续运行

方法 2：

可以直接在：我的电脑 - 管理 - 服务 中寻找到该 LdapService，可以对其进行开启和关闭

2.3.2 LDAP 添加条目

添加文件的后缀为 LDIF 格式，并将添加好的空文件放到 openLdap 的安装路径中，并用文件编辑器打开填入内容。

例如：单击鼠标右键添加一个 test.txt 文件，并将其后缀修改为 ldif （即 test.ldif ）后用自己喜欢的文档编辑器将其打开。

下面是一个 test.ldif 的文件实例。

```
dn: ou=fanvil, dc=beijing,dc=com
ou: fanvil
```

```
objectClass: organizationalUnit

dn: ou=organizationalRolemun, ou=fanvil, dc=beijing,dc=com
ou: organizationalRolemun
objectClass: organizationalUnit

dn:         cn=bingwang1,ou=organizationalRolemun,         ou=fanvil,
dc=beijing,dc=com
telephoneNumber: 8231
registeredAddress: WWWEEE
objectClass: organizationalPerson
telexNumber: 8110
postalAddress: 332211
sn: bing
street: Zqq
cn: bingwang1

dn:        cn=zhangqiang1,ou=organizationalRolemun,        ou=fanvil,
dc=beijing,dc=com
telexNumber: 2000
street: Zqw
sn: zhang
telephoneNumber: 2000
ou: 3ou
objectClass: organizationalPerson
postalAddress: 334411
registeredAddress: ACXCXCCXC
cn: zhangqiang1

dn:         cn=sunliang,ou=organizationalRolemun,         ou=fanvil,
dc=beijing,dc=com
telephoneNumber: 123333
registeredAddress: WEEWEWEE
objectClass: organizationalPerson
telexNumber: 6564
sn: sun
cn: sunliang
```

```
dn:          cn=zhangchao,ou=organizationalRolemun,          ou=fanvil,
dc=beijing,dc=com
telephoneNumber: 7777
registeredAddress: ZZZWWW
objectClass: organizationalPerson
telexNumber: 54646
sn: zhang
street: XAZ
cn: zhangchao

dn: cn=xieqian,ou=organizationalRolemun, ou=fanvil, dc=beijing,dc=com
telephoneNumber: 3312123
registeredAddress: XXXZZZ
objectClass: organizationalPerson
telexNumber: 242342
postalAddress: 332221
sn: xie
cn: xieqian
```

注意：各行中首尾不能出现空格，如果格式有问题会报错

1.点击 开始 - 运行。

2.输入 cmd，进入命令行界面。（如果 window10 没有找到运行，可以直接输入 win + r 后输入 cmd）

3.进入对应的 LDAP 安装的路径，例如我这里的路径是 C:/work/openLdap，（如果条件允许，建议不安装在 C 盘中，且路径为纯英文）并输入执行命令：slapadd -v -l ./test.ldif

注意：slapadd 命令只能对本地的 LDAP 服务进行操作，操作时本地 LDAP 服务必须先停止。

LDAP 中常用属性：

DN：Distinguished Name，可以叫做条目区分名。在一个目录中这个名称总是唯一的，也是用来标识一个节点的主要方式。它有若干属性：

1.CN=Common Name 为用户名或服务器名，最长可以到 80 个字符，可以为中文；

2.OU=Organization Unit 为组织单元，最多可以有四级，每级最长 32 个字符，可以为中文；

3.DC= Domain Component 为目录结构

4.O=Organization 为组织名，可选，可以 3—64 个字符长

2.3.3 关于 LDAP 中的 Schema

LDAP 中，schema 用来指定一个目录中所包含的 objects 的类型（objectClass）以及每一个 objectClass 中的各个必备（mandatory）和可选（optional）的属性（attribute）。因此，Schema 是一个数据模型，它被用来决定数据怎样被存储，被跟踪的数据的是什么类型，存储在不同的 Entry 下的数据之间的关系。schema 需要在主配置文件 slapd.conf 中指定，以用来决定本目录中使用到的 objectClass。管理员可以自己设计制定 schema，一般包括属性定义（AttributeDefinition）、类定义（ClassDefinition）以及语法定义（SyntaxDefinition）等部分。
创建好 schema 文件后，将做好的 schema 文件拷贝到 ldap 的 schema 目录下。然后修改 slapd.conf 文件，将新的 schema 文件加入申明。
如果关于创建和 Schema 还有其他问题，可参考相关网络资料。

2.4 图形化管理工具

2.4.1 LDAPBrowser 介绍

关于 LDAPBrowser,是一个支持在 windows 系统上运行的 LDAP 图形化管理工具。可以对 LDAP 数据进行浏览，修改，和管理 LDAP 上的联系人条目信息。

2.4.2 LDAPBrowser 下载及安装

下载 jdk1.4 或 jdk1.5 或更高的版本（安装及配置环境变量等步骤可以在网上搜索相关资料）下载 LdapBrowser：
http://www.blogjava.net/Files/Unmi/LdapBrowser282.rar
LdapBrowser 无需安装，可直接使用。点击安装目录下的 lbe.bat 即可执行 LdapBrowser。

2.4.3 添加初始数据

点击安装目录下的 lbe.bat 后，弹出下面的选项，选择 Edit 对其进行操作或选择 New 新建一个 Session List。如图 2-4-1

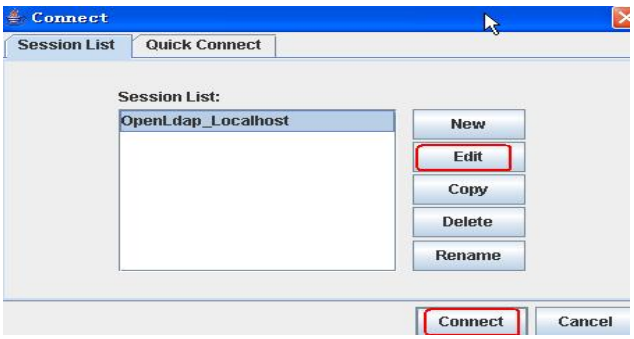

图 2-4-1

下面是对各个输入框或选择框进行介绍:

Host:输入 openLdap 主机名或 IP，点击 Fetch DNs 则会自动匹配到 openldap 在 slapd.conf 配置的根域

Port：是系统默认预留的端口

Version:是版本，默认为 3

这里需要勾选 append base DN

User DN：这里我们填写的是 cn=manager 是 openldap 安装时的管理员账号。

Password：是我们修改过的密码,如果没有修改密码，密码默认为安装时的初始密码：secret

然后点击保存，回到连接界面点击 connet。如果需要匿名登录，则选中 Anonymous bind，需要说明的是，匿名登录只能查看数据。如图 2-4-2

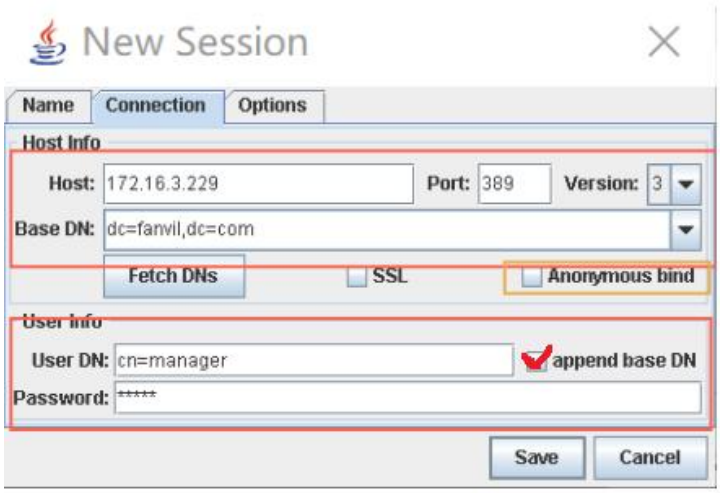

图 2-4-2

填写信息完成后如下图 2-4.3 所示：

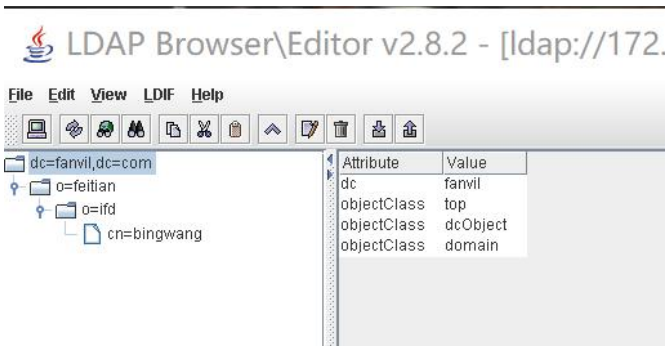

图 2-4-3

2.4.4 添加目录属性

下面就拿一个有数据的 ldap 进行举例：

如果需要为一个元素增加 Attribute，按如图 2-4-4，2-4-5，2-4-6 操作：

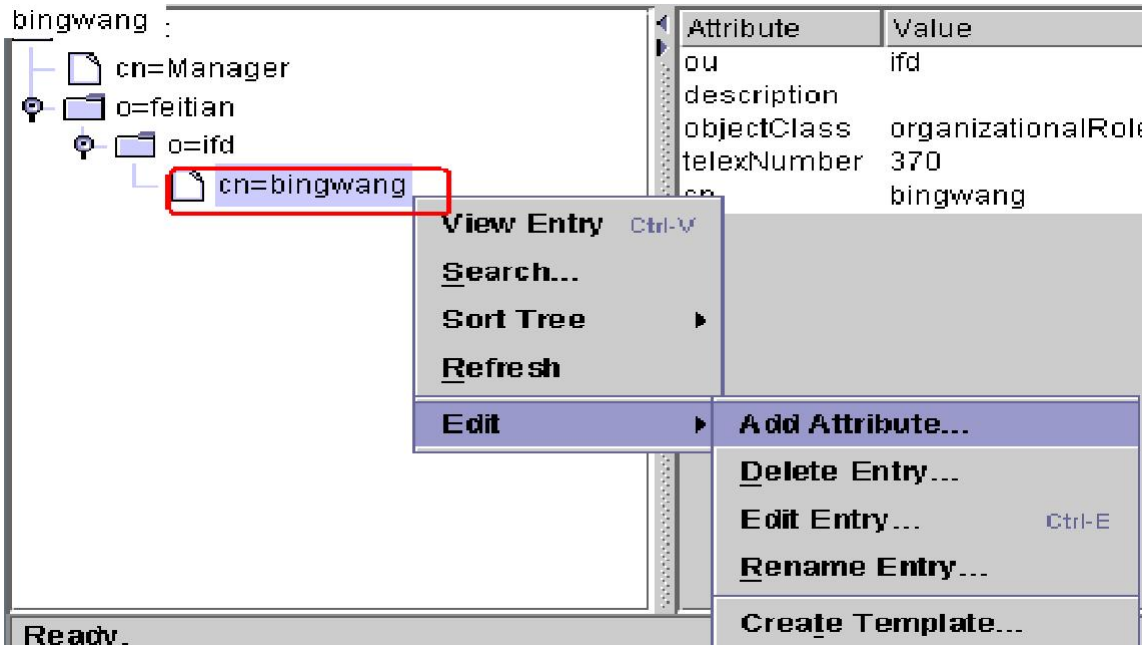

图 2-4-4

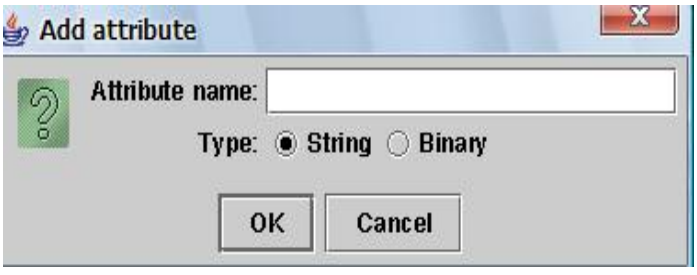

图 2-4-5

图 2-4-6

最后点击 Apply 完成 Attribute 增加。需要注意的是增加的属性名称一定是符合 ldap 标准的，或者自定义增加的，否则将会增加失败，如图 2-4-6 增加属性 a 则不能成功。具体 ldap 有哪些默认的属性值可以参考%openldap_home%\schema\core.schema 文件。

2.4.5 删除目录属性

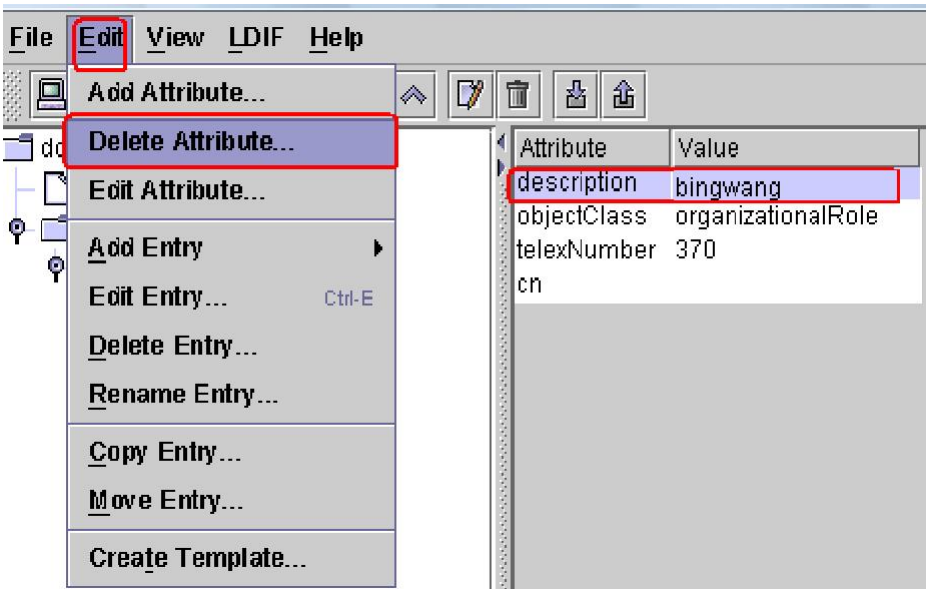

图 2-4-7

选中一个元素的 Attribute，使用删除 Attribute 操作。如上图 2-4-7

2.4.6 修改目录属性

在目录的属性上双击即可弹出修改的界面，输入新的属性值点击【Apply】即可完成属性的属性值更改。

2.4.7 增加目录

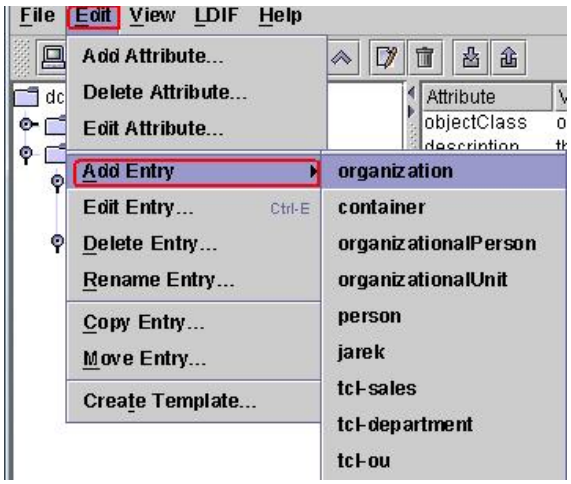

图 2-4-8

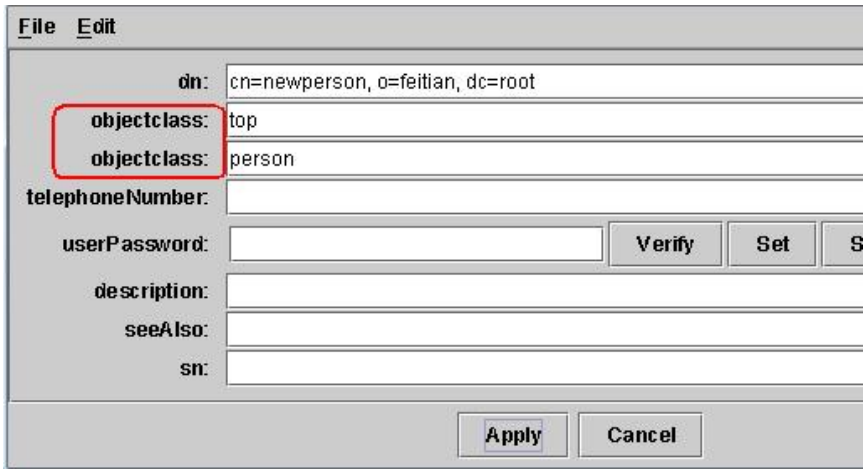

图 2-4-9

2.4.8 修改目录

修改目录是针对目录的所有属性进行修改，可以参照上面的修改目录属性操作，也可以通过下面的操作. 如图 2-4-10

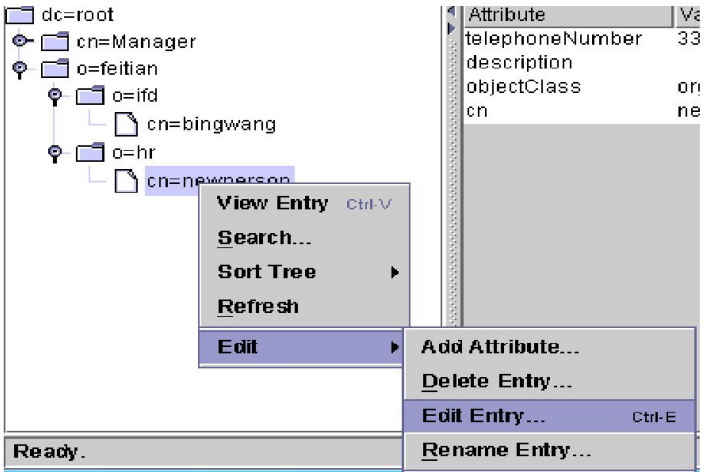

图 2-4-10

2.4.9 删除目录

先选中要删除的目录，然后进行下图 2-4-11 操作

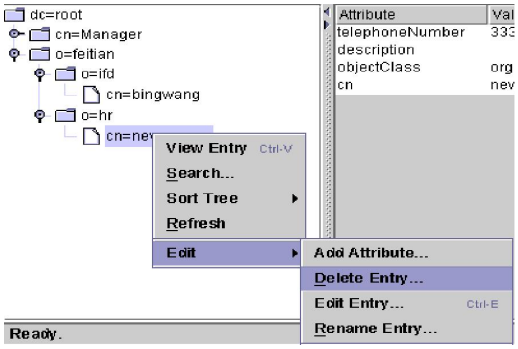

图 2-4-11

2.4.10 实例

下面列举一个实例来理解 LDAP 数据的树状结构。如图 2-4-12

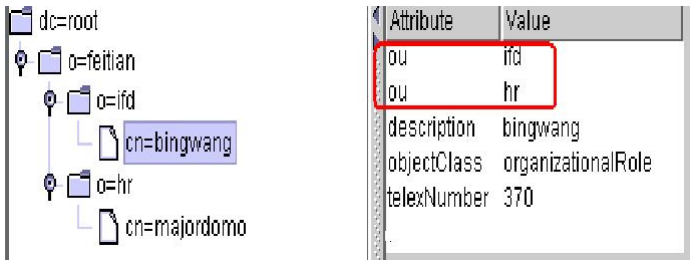

图 2-4-12

通过图 2-4-12 可以看出 cn=bingwang 这个实体在最末端，它的完整 DN 是什么呢？

dn:cn=bingwang,o=ifd,o=feitian,dc=root。

可见最顶端的根节点在表达式中写在最后的位置，其它依次类推。这里讲述的是节点的 dn.如果节点本身还需要附加一些属性来丰满内容，attribute 将会带来很大的实用性。比如通讯录的某个人是个节点，那么人员的地址、电话号码等就可以作为 attributes。图 2-4-12 举例表示了用户 bingwang 的若干属性，其中 ou 属性两个，分别表示用户在 ifd 部门和 hr 部门任职。由此可见，attribute 是可以一对多(一个节点多个相同属性，值各不同)。因此 attributes 可以充分运用于描述节点的各类信息。下面附带图 2-4-12 节点 cn=bingwang 的 ldif

```
dn: cn=bingwang, o=ifd, o=feitian, dc=root
ou: ifd
ou: hr
description:bingwang
objectClass: organizationalRole
telexNumber: 370
cn: bingwang
```

3 Microsoft Active Directory

3.1 下载并安装 Microsoft Active Directory

3.1.1 Microsoft Active Directory 介绍

活动目录（Active Directory）是面向 Windows Standard Server、Windows Enterprise Server 以及 Windows Datacenter Server 的目录服务。

3.1.2 在 windows server 2008r2 下安装 Microsoft Active Directory

在 windows server 2008r2 系统下安装 Microsoft Active Directory

1.在 运行 - cmd 中，输入 dcpromo.如图 3-1-1

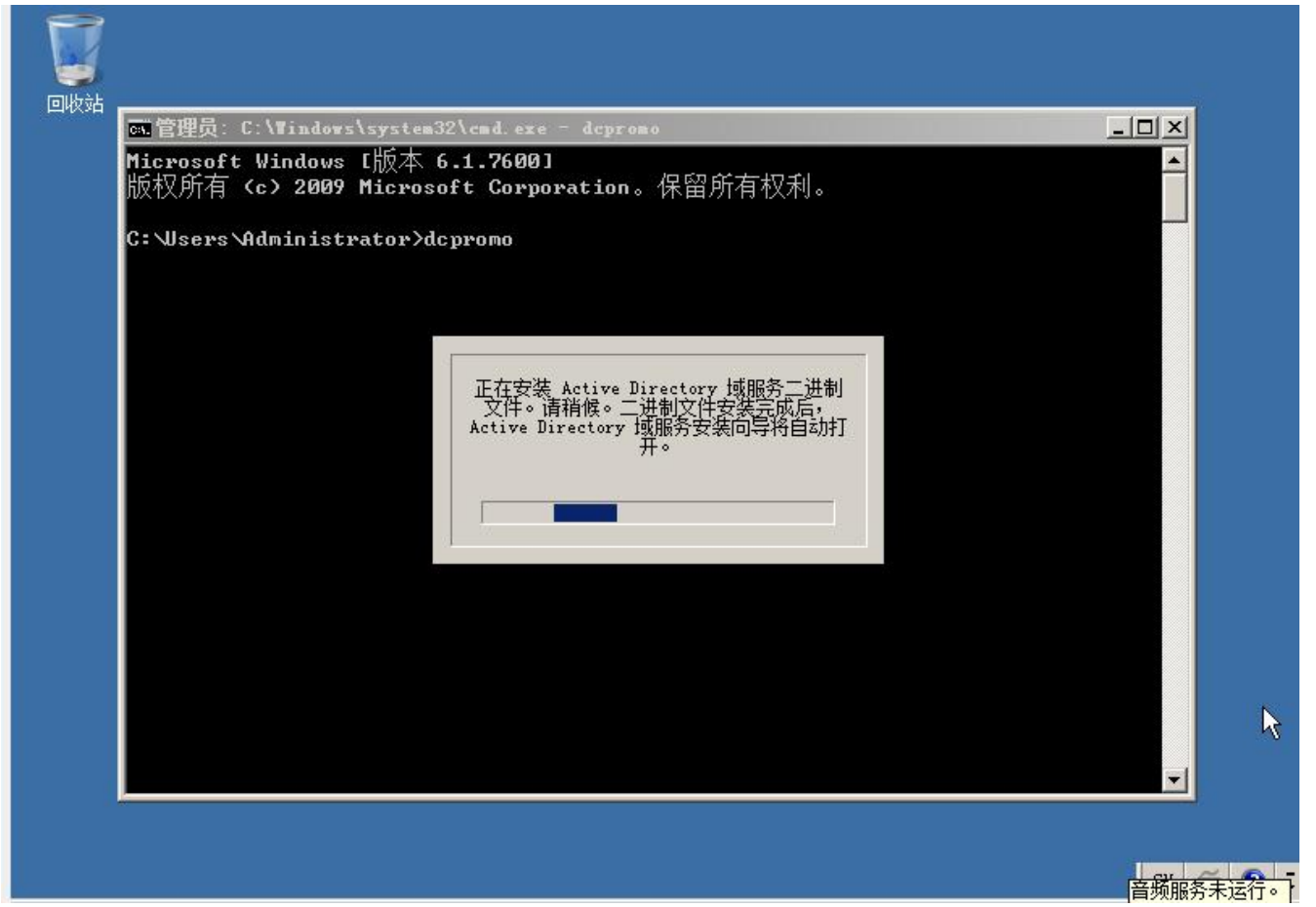

图 3-1-1

2.在等待一段时间后，Active Directory 的安装向导出现，我们在阅读说明后点击下一步.如图 3-1-2

图 3-1-2

3.阅读说明后点击下一步。如图 3-1-3

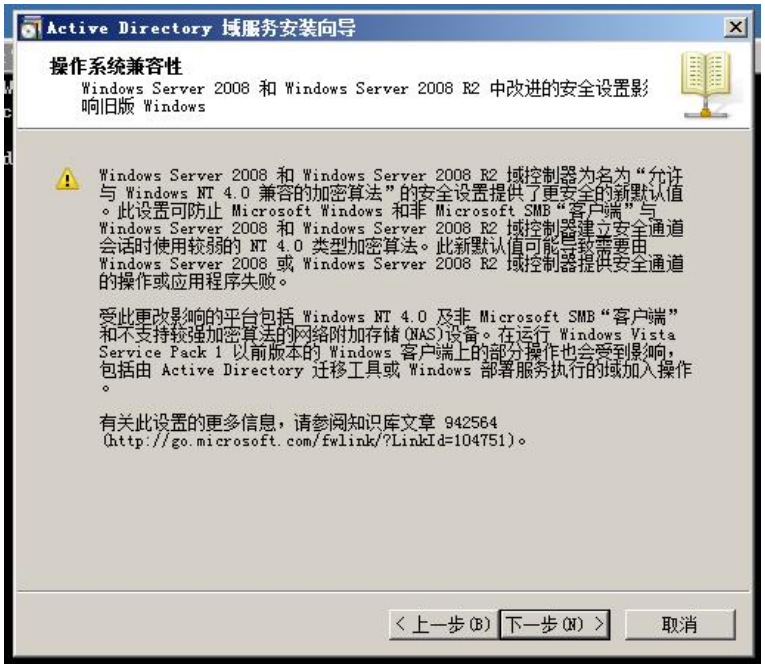

图 3-1-3

4. 这里我们选择在新林中新建域，点击下一步。如图 3-1-4

图 3-1-4

5. 输入新目录林根域的完全限定的域名。例如：下图中输入的 ldap.fanvil.com 点击下一步. 如图 3-1-5

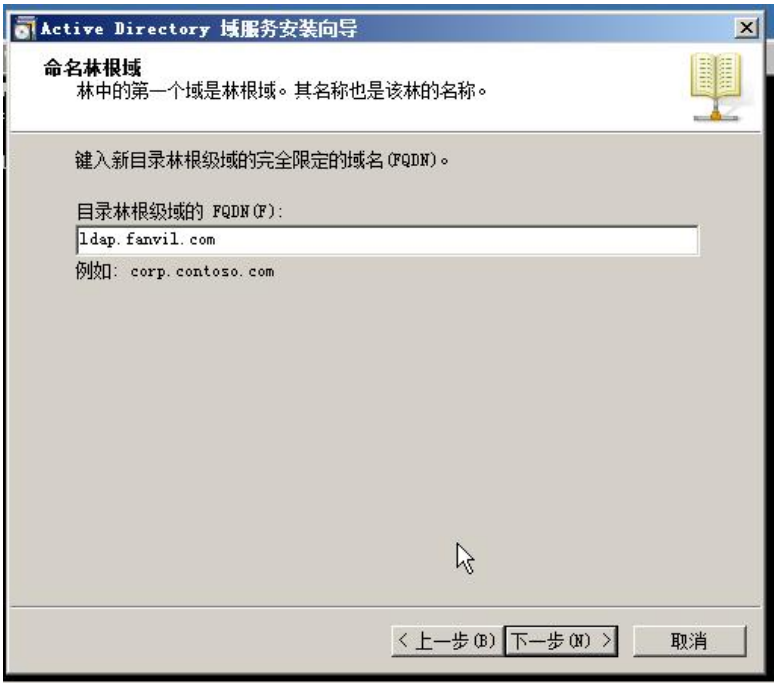

图 3-1-5

安装向导将检查该域名是否在本地网络中使用. 如图 3-1-6

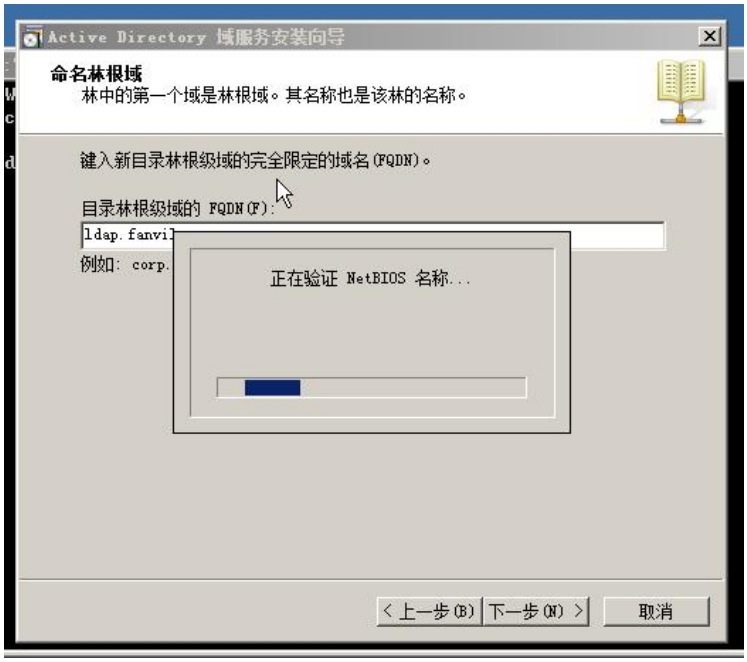

图 3-1-6

6. 在林功能级别的下拉列表中选择所需林功能级别，并单击下一步。如图 3-1-7 有关更多信息，请单击“域和林功能级别”

图 3-1-7

7. 在域功能级别的下拉列表中选择所需林功能级别，并单击下一步。如图 3-1-8 有关更多信息，请单击“域和林功能级别”

图 3-1-8

注意：如果您选择的是 Windows Server 2008 R2 的林功能级别，您将不会提示选择域功能级别。

8. 如果需要，为该域控制器选择其他选项，并单击下一步。如图 3-1-9

图 3-1-9

注意：如果没有分配一个静态 IP 给服务器，可能会收到下图的警告，可以设置一个静态的网络给服务器，如果有问题，可以在网络上查找相关的配置方法或者联络贵公司的网络管理员。（这里选择否，再进行静态 ip 的设置）

如图 3-1-10

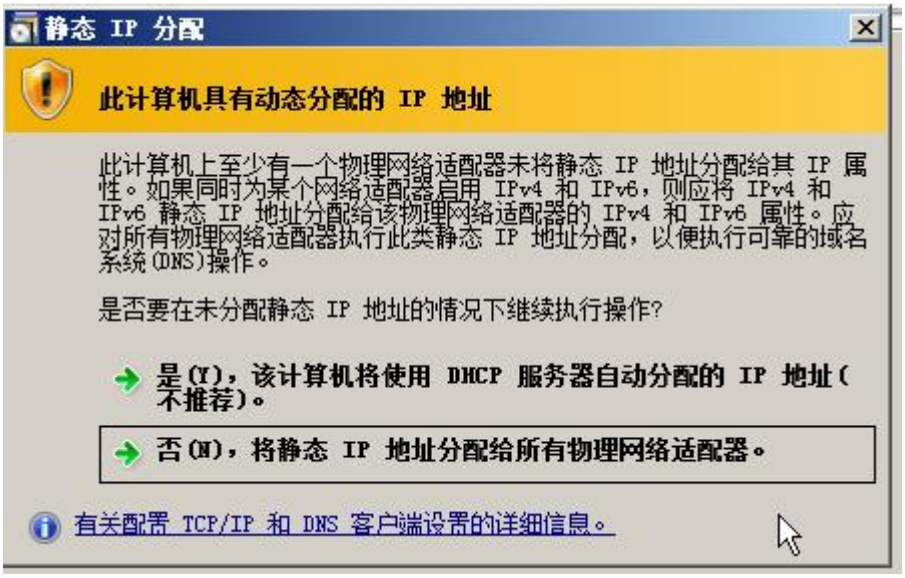

图 3-1-10

9. 向导将提示 DNS 委托。由于还没有配置任何 DNS，您可以忽略该消息并单击 Yes.

如图 3-1-11

图 3-1-11

10. 为数据库、日志文件和 SYSVOL 文件夹指定所需的路径，并单击 Next

如果有任何疑问，可以点击”放置 Active Directory 域服务文件”进行查询.

如图 3-1-12

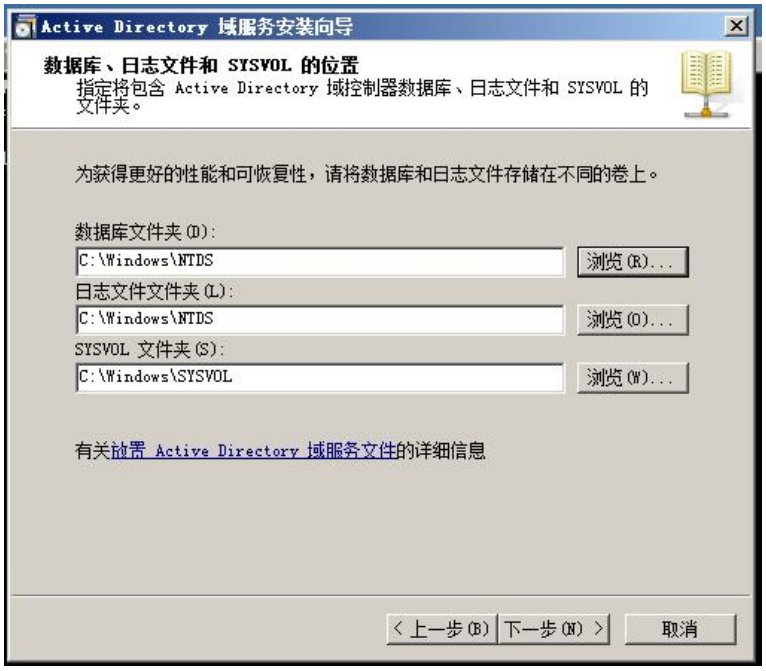

图 3-1-12

11.为 active directory 恢复模式配置密码，然后单击 Next。有关更多信息，请单击目录服务还原模式密码。

这里提及选择一个强密码，即大于等于 7 个字符的。例如：这里我将密码设置为 Qq123456，您可以设置您喜欢且满足条件的密码，但是该密码一定要进行记录，不能忘记。如图 3-1-13

图 3-1-13

12.这里列出了配置后的信息，在核对无误后，点击 next。

如果信息有误可以点击上一步进行更改，如果有任何问题，可以点击”使用应答文件”进行查看.如图 3-1-14

图 3-1-14

在完成上述操作后，计算机将开始进行创建 Active Directory。这个过程时间视硬件性能而定。如图 3-1-15

图 3-1-15

13. 点击”完成”按钮。 如图 3-1-16

图 3-1-16

3.2 安装 Active Directory Lightweight Directory Services Role

3.2.1 在 windows server 2008r2 下安装 Active Directory Lightweight Directory Services Role

1. 点击 开始 - 管理工具 - 服务器管理器
2. 右键点击 角色 ，选择添加角色。如图 3-2-1

图 3-2-1

3.弹出下面的对话框，单击下一步。如图 3-2-2

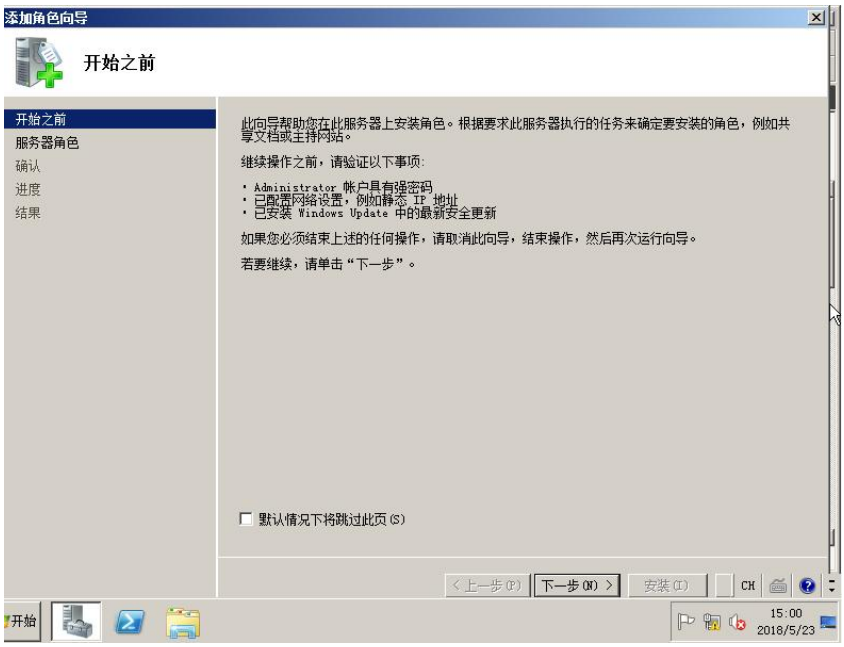

图 3-2-2

4.在下面的角色中找到我们要安装的 Active Directory 轻型目录服务，并将其勾选，点击下一步。如图 3-2-3.如果对该角色有任何问题，可以点击 Active Directory 轻型目录服务（AD LDS）进行了解。

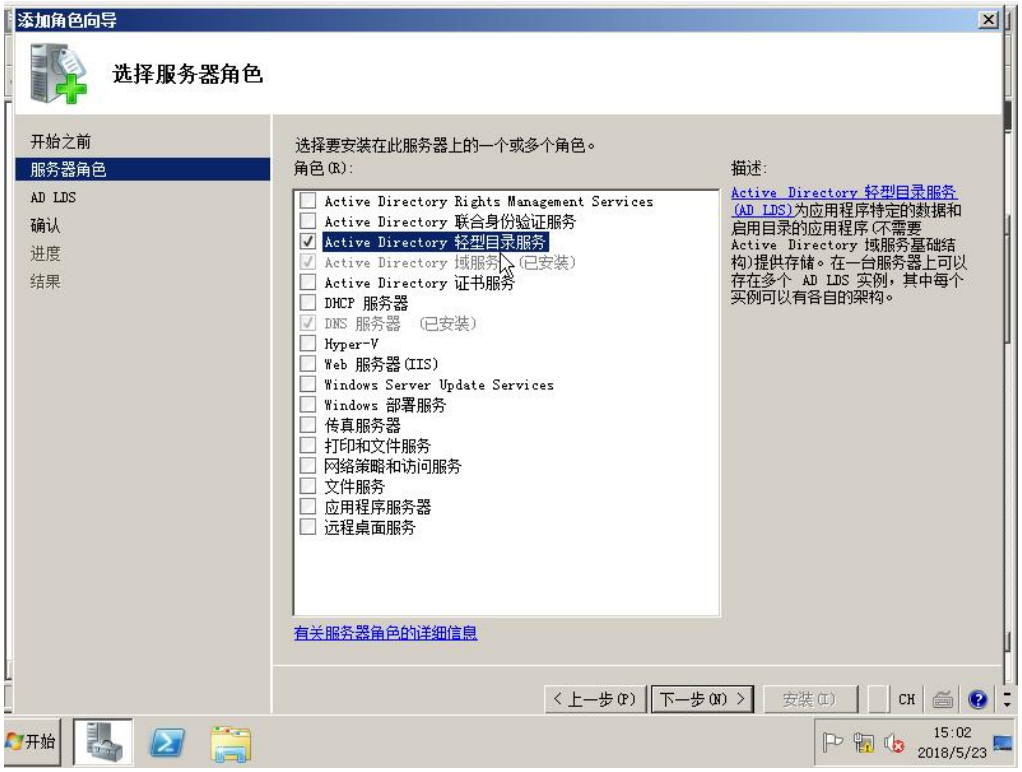

图 3-2-3

5.一直选择下一步，选择默认的配置。

6. 当安装完成，点击关闭。如图 3-2-4

图 3-2-4

安装成功后，找到 Active Directory 轻量级目录。

服务器管理器角色中列出的服务角色。如图 3-2-5

图 3-2-5

3.3 配置 Microsoft Active Directory Server

3.3.1 配置 Microsoft Active Directory Server

在这里，您可以逐条的添加条目，修改或是删除条目，也可以通过下一小节的工具进行多条目的导入。

向 Active Directory 中添加一个条目：

1. 点击 开始 - 管理工具 - 服务器管理器

2. 展开 角色 - 展开 Active Directory 域服务 - 展开 Active Directory 用户和计算机

3. 右键单击刚才创建的域名 - 新建 - 组织单位。如图 3-3-1

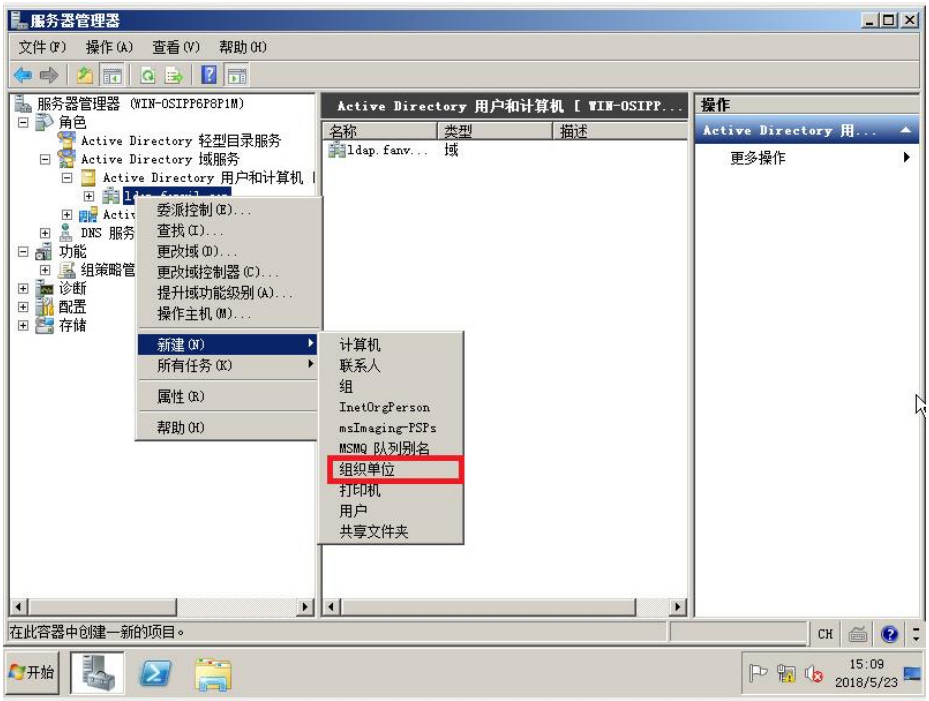

图 3-3-1

4. 填写一个组织单位的名称。例如：这里填写的是 fanvil，您也可以填写任何名称。如图 3-3-2

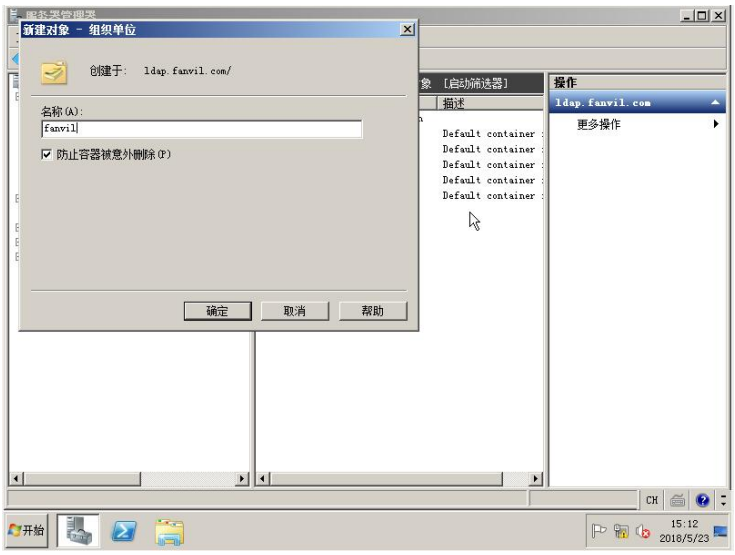

图 3-3-2

5. 点击确定保存修改。

6. 右键单击刚才创建的组织单位 - 新建 - 联系人。如图 3-3-3

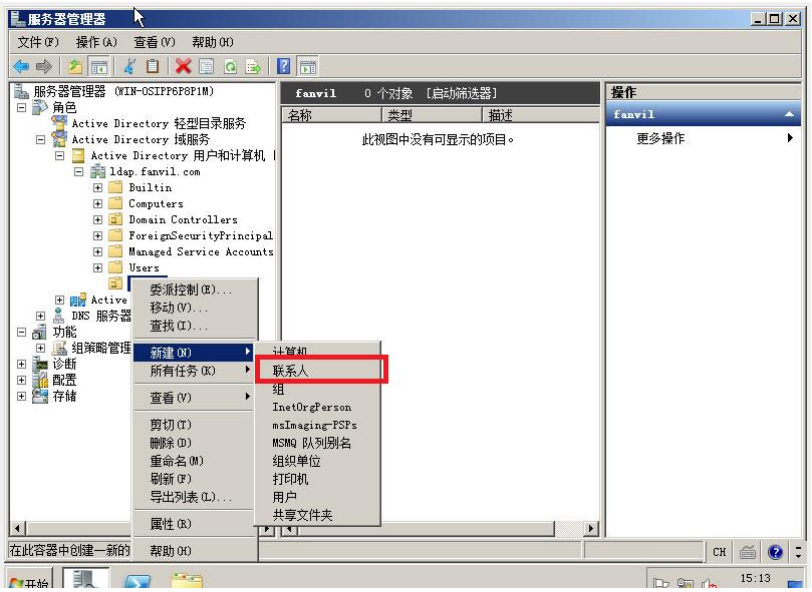

图 3-3-3

7. 将信息填入字段中。如图 3-3-4

图 3-3-4

8. 点击确定保存修改。

9. 双击刚才添加的联系人，进行进一步的信息填写。如图 3-3-5

图 3-3-5

完成后点击确定保存修改。这样一条联系人信息添加成功。您也可以重复操作对联系人信息进行修改。

3.4 添加条目

有时需要批量地向 AD 域中添加用户帐户，这些用户帐户既有一些相同的属性，又有一些不同属性。如果在图形界面逐个添加、设置，那么需要的时间和人力会超出能够承受范围。一般不超过 10 个，我们可利用 AD 用户帐户复制来实现。如果超过，就应考虑使用命令行工具，来实现批量导入导出对象。微软默认提供了两个批量导入导出工具，分别是 CSVDE(CSV 目录交换)和 LDIFDE(LDAP 数据互换格式目录交换)。

具体选择上述哪个工具取决于需要完成的任务。如果需要创建对象，那么上述两个工具均可使用。如果需要修改或删除对象，则必须使用 LDIFDE。

3.4.1 使用 Ldifde 向 Active Directory 添加条目

你可以创建一个 ldif 格式的文件来批量导入 Active Directory 条目。
创建一个新的文本文档，然后将扩展名 txt 改为文件扩展名 ldif。例如：创建一个示例文件 test.ldif 文件，下面为示例信息：

```
##Create a new organizational unit##
dn: OU=fanvil2,DC=ldap,DC=fanvil,DC=com
changetype: add
objectClass: top
objectClass: organizationalUnit
ou: fanvil2
name: fanvil
##create a new contact##
dn: CN=liang zhang,OU=fanvil2,DC=ldap,DC=fanvil,DC=com
changetype: add
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: contact
cn: liang zhang
sn: zhang
```

```
givenName: liang
initials: zl
name: liang zhang
ipPhone: 1322
mobile: 3322445566
```

导入 test.ldif 文件：

1.点击 开始 - 运行

2.输入 cmd 进入命令行界面。

3.使用 cd 命令移动到 test.ldif 文件的目录

4.输入 ldifde -i -f test.ldif 导入文件。如果导入成功，可以看到屏幕上提示“成功的添加了 n 个条目”(此处的 n 代表 n 条信息)如图 3-4-1

图 3-4-1

3.4.2 使用 Csvde 工具向活动目录添加条目

除了上面提到的 ldif 文件，我们还可用.CSV 格式的文件对条目进行批量导入。创建一个表格类应用（比如：Excel）的文档，然后保存。

例如:在本次测试中我们创建一个Excel 表格,将其后缀改为.CSV 即 test3.CSV。文件中信息如图 3-4-2：

	A	B	C	D	E	F
1	DN	objectClass	ou	cn	sn	ipPhone
2	ou=fanvil3,dc=ldap,dc=fanvil,dc=com	organizationalUnit	fanvil3			
3	cn=a b,ou=fanvil2,dc=ldap,dc=fanvil,dc=com	contact		a b	a	123

图 3-4-2

导入 test3.csv 文件

1.点击 开始 - 运行

2.输入 cmd 进入命令行界面。

3.使用 cd 命令移动到 test3.csv 文件的目录

4.输入 csvde -i -f test.csv 导入文件。如果导入成功，可以看到屏幕上提示“成功地修改了 n 个目录”(此处的 n 代表 n 个条目)如图 3-4-3

图 3-4-3

3.5 创建用户账户

1. 点击 开始 - 管理工具 - 服务器管理器

2. 展开 角色 - 展开 Active Directory 域服务 - 展开 Active Directory 用户和计算机

3. 右键单击刚才创建的域名 - 选择新建 - 用户。如图 3-5-1

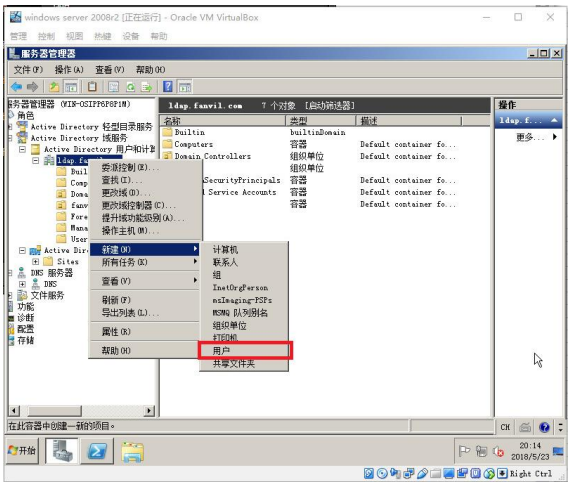

图 3-5-1

4. 进入后填入信息，点击下一步. 如图 3-5-2

图 3-5-2

5. 填写密码，如有其它需要也可进行配置，之后点击下一步. 如图 3-5-3，这里可以选择密码永不过期选项，管理员也可以将配置配为用户不能更改密码。

图 3-5-3

6. 可以看到创建用户的信息，如果无误点击完成。如果信息与预期不符可点击上一步进行修改。如图 3-5-4

图 3-5-4

3.6 关于话机及相关配置

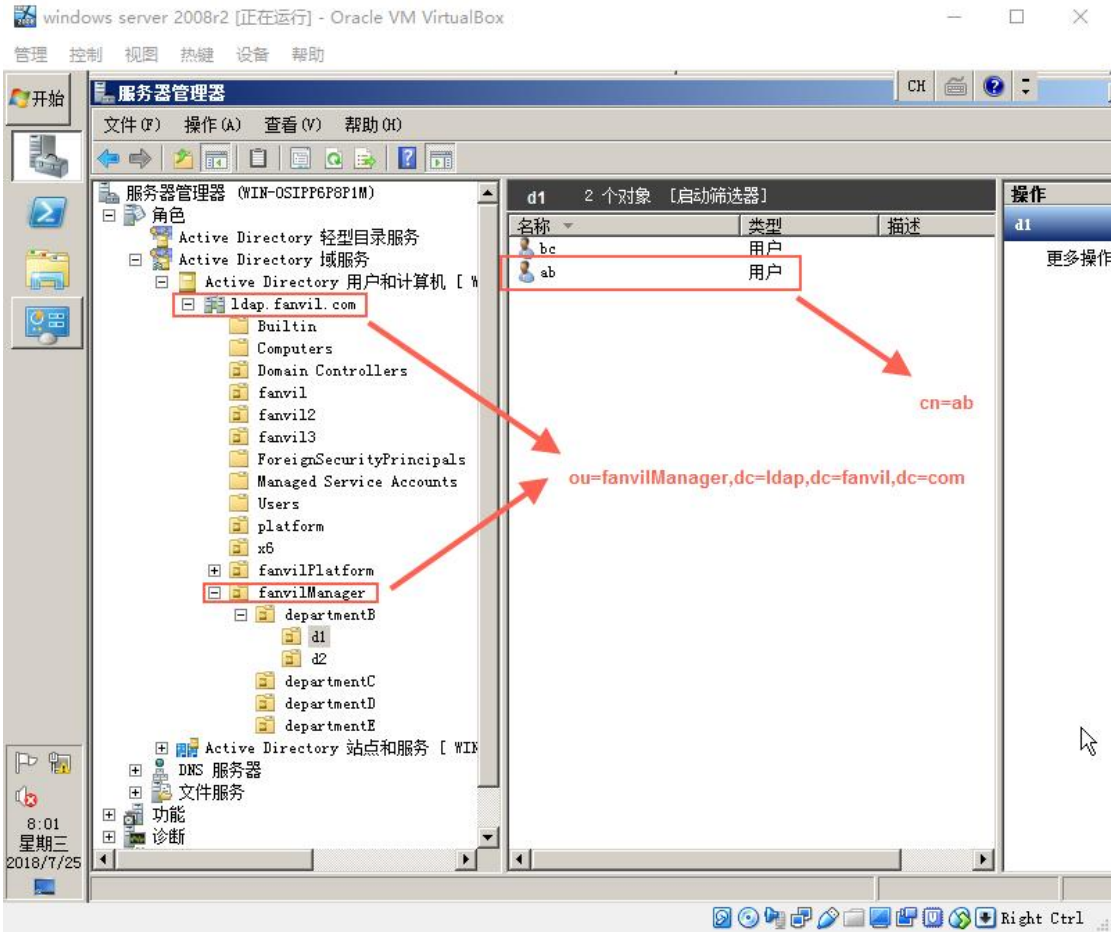

图3-6-1

这里可以在域 ldap.fanvil.com 中创建一个组织用户来管理我们的 ldap 电话本。

以图中的举例,我们可以在域 ldap.fanvil.com 下创建一个 fanvilManager 的组织单位来当做 ldap 的根节点，方便管理，再在该节点下创建出各个部门的组织单位，再向其中添加联系人。关系如图 3-6-2.

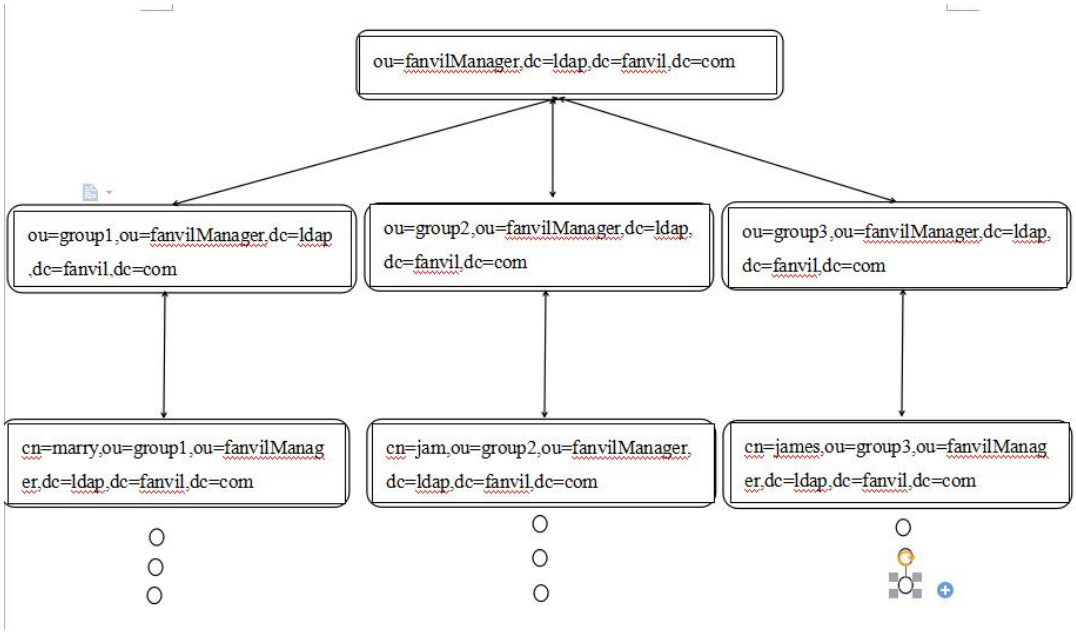

图 3-6-2

该处配置配好后，在话机网页端进行配置。如图 3-6-3

图 3-6-3

关于其他配置的填写，如办公电话等，active directory 为我们提供一些选择，对应的常用属性名如下：

图 3-6-4

对应编号	选项卡对应项名	属性名
1	姓	sn
2	名	givenName
3	显示名称	displayName
4	描述	description
5	办公室	physicalDeliveryOfficeName
6	英文缩写	initials
7	电话号码	telephoneNumber
8	电子邮件	mail
9	网页	wWWHomePage
10	电话号码其他	otherTelephone
11	网页其他	url

图 3-6-5

对应编号	选项卡对应名称	属性名
1	家庭电话	homePhone
2	寻呼机	pager
3	移动电话	mobile
4	传真	facsimileTelephoneNumber
5	IP 电话	ipPhone
6	注释	info
7	家庭电话-其他	otherHomePhone
8	寻呼机-其他	otherPager
9	移动电话-其他	otherMobile
10	传真-其他	otherFacsimileTelephoneNumber
11	IP 电话-其他	otherIpPhone

图 3-6-6

对应编号	选项卡对应项名	属性名
1	公司	company
2	部门	department
3	职务	title
4	经理-姓名	manager
5	直接下属	directReports

在配置好一个用户后，我们可以通过 simple 方式来登录我们的电话本，例如在上文中，我创建的：登录名为 ldapuser1@ldap.fanvil.com,密码为 Qq123456。话机网页端配置如图 3-6-7：

图 3-6-7

关于配置项：办公电话，移动电话，和其他三个配置项：

您可以随意的配置您所希望查询到的信息，通过上文中信息中所对应的属性。如：

我们可以在办公电话一栏填写如 电话号码，寻呼机号码，家庭号码，iP 号码等等，只要服务器端填写了相应的信息，您就可以查询到它。移动电话一栏和其他一栏也是如此。

如图 3-6-8

图 3-6-8

在这里，我按照上面的属性名，将办公电话字段配置为：电话号码：telphoneNumber，移动电话：mobile 和家庭电话：homePhone。那样，我们在话机上对应的栏中就能看到对应服务器上配置的电话号码，移动电话和家庭电话的值。其他配置，在下面的章节会有介绍，这里不再介绍。

4 在 linux 搭建 openLdap

4.1 安装总述

现在在以 linux 为系统的服务器中，一般都使用 openLdap 来搭建 ldap 服务器。下面对所需库和注意事项进行总述。

4.1.1 Berkeley DB

Berkeley DB 是由美国 Sleepycat Software 公司开发的一套开放源代码的嵌入式数据库管理系统（已被 Oracle 收购），它为应用程序提供可伸缩的、高性能的、有事务保护功能的数据管理服务。
由于 openldap 需要 Berkeley DB 来存放数据，所以需先安装 Berkeley DB。安装
注意：这里所选用的 DB.tar 版本需要预先与要下载的 openldap 版本进行一下确认，需要在特定版本下二者才能正常使用。
例如：openldap-2.4.44 要求用 Oracle Berkeley 4.4-4.8 或者 5.0-5.1 版本的。
如果在下面安装 openldap 的时候遇到下面的报错，一般都是因为这个原因导致的。

Error：BerkeleyDB version incompatible with BDB/HDB backends

4.1.2 Cyrus -sasl

SASL 的全称为 the Simple Authentication and Security Layer.它的机制是对协议执行验证。如果有某种服务（比如 SMTP 或我们现在所要搭建的 ldap）使用了 SASL，这种协议的应用程序之间将会共享代码。

4.1.3 openLdap

openldap 是本次的主角，在上文中已经详细介绍，这里不再过多叙述。这里唯一需要重申的一点是在上文 Berkeley DB 中提及的版本不兼容性的问题，在安装之前一定要查明所要安装的版本。

4.2 安装

本次使用的是 Ubuntu 12.04.1。您也可以查看自己的 linux 虚拟机版本通过命

令：

```
#cat /etc/issue
```

之后的安装要按照文档的顺序进行

注意：最好使用 root 用户进行下面的安装操作

4.2.1 安装 Cyrus -sasl

下载 cyrus-sasl 并安装。在进行这一步之前可以预先进到自己创建的目录里再进行安装

这里我们选择的版本是 2.1.25 版本

```
#wget http://ftp.andrew.cmu.edu/pub/cyrus-mail/cyrus-sasl-2.1.25.tar.gz
```

之后我们会看到如图 4-2-1 的下载界面。

注意：请确保您的虚拟机当前可以连接上网络。如果您所输入的资源不正确，可能会出现下图上半部分提示的 404 问题。

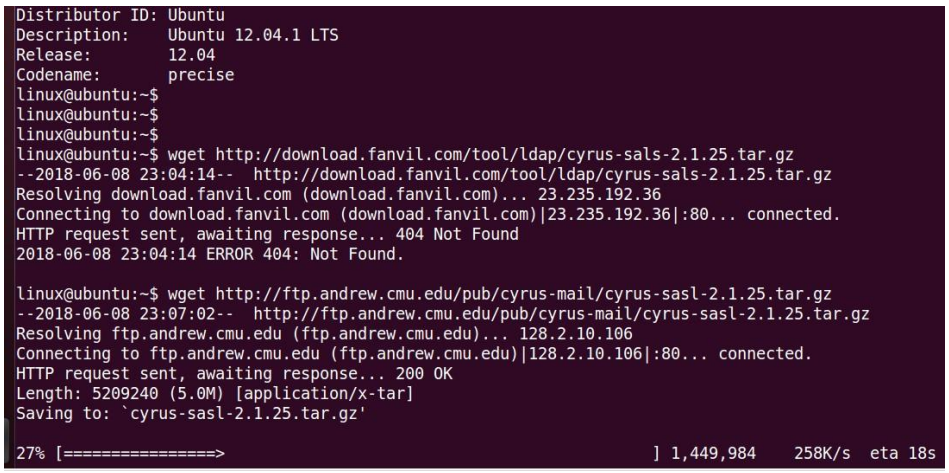

图 4-2-1

解压，输入如下命令解压我们刚下好的安装包

```
#tar xzvf cyrus-sasl-2.1.25.tar.gz
```

解压成功后我们可以看到如图 4-2-2 的效果

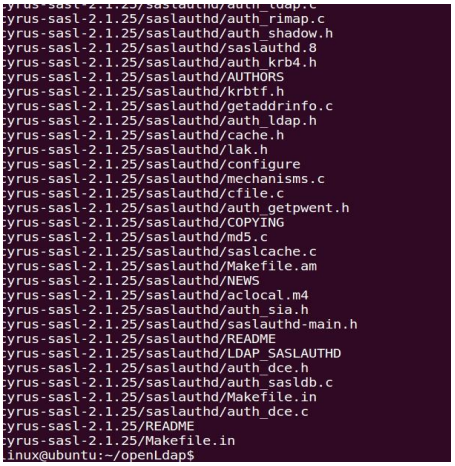

图 4-2-2

进入到刚解压好的文件中后进行配置操作，输入指令进行配置.如图 4-2-3

```
#cd cyrus-sasl-2.1.25
#./configure  -prefix=/usr/local/sasl2  -with-dblib=no  -without-des
  -with-openssl=/usr/local/ssl
```

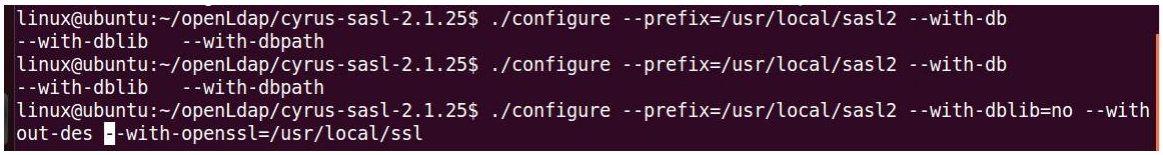

图 4-2-3

配置完成后会提示输入 make，在看到图 4-2-4 的提示后我们输入 make

```
#make
```

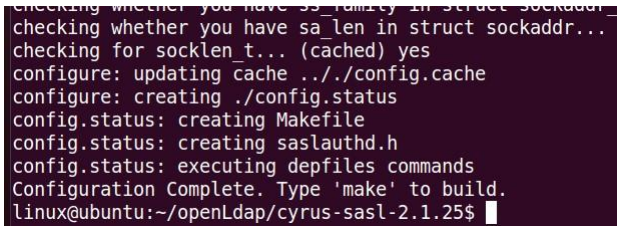

图 4-2-4

在看到如图 4-2-5 的显示后输入 make install

```
#make install
```

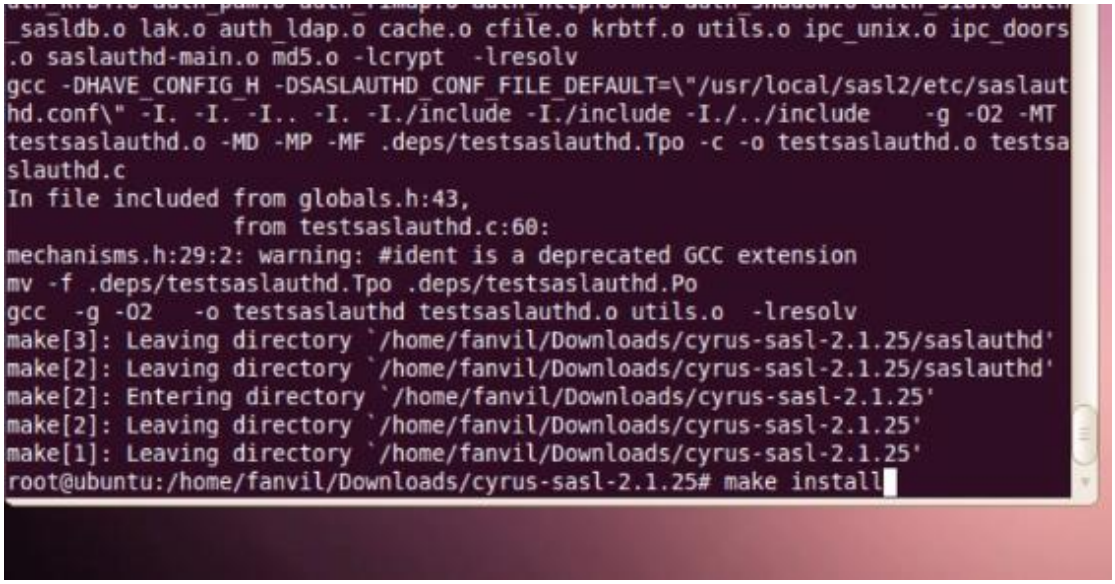

图 4-2-5

之后我们配置库文件搜索路径，如果不配该路径，在执行可执行文件的时候可能会出现搜索不到路径的情况。错误提示例如：

```
Error：while loading shared libraries
```

如果在过程中出现这个问题，可以在参考资料 2 中查看该问题。

配置库文件搜索路径，输入：

```
#echo "/usr/local/sasl2/lib" >> /etc/ld.so.conf
#echo "/usr/local/sasl2/lib/sasl2" >> /etc/ld.so.conf
#ldconfig -v
```

把原有的 sasl 文件替换掉

```
# cd /usr/lib
# mv libsasl2.so libsasl2.so.OFF
# mv libsasl2.so.2.0.23 libsasl2.so.2.0.23.OFF
# mv lIbsasl2.so.2 libsasl2.so.2.OFF
# ln -s /usr/local/sasl2/lib/* /usr/lib
# ln -s /usr/local/sasl2/lib/sasl2 /usr/lib/sasl2
# ln -s /usr/local/sasl2/lib/libsasl2.so.2.0.23 /usr/lib/libsasl2.so.2
# ln -s /usr/local/sasl2/lib/libsasl2.so /usr/lib/libsasl2.so
```

4.2.2 安装 BerkeleyDB

这里我们选择的版本是 4.6.21

下载好后输入命令解压文件，并进入到文件夹 build_unix 下。如图 4-2-6

```
#tar xzvf db-4.6.21.tar.gz
#cd db-4.6.21/build_unix
```

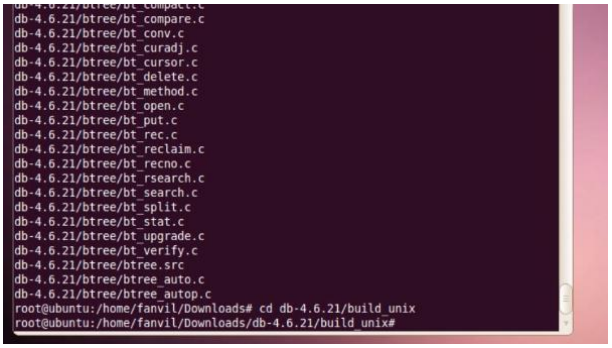

图 4-2-6

配置依赖环境.如图 4-2-7

```
#../dist/configure  -prefix=/usr/local/BerkeleyDB
```

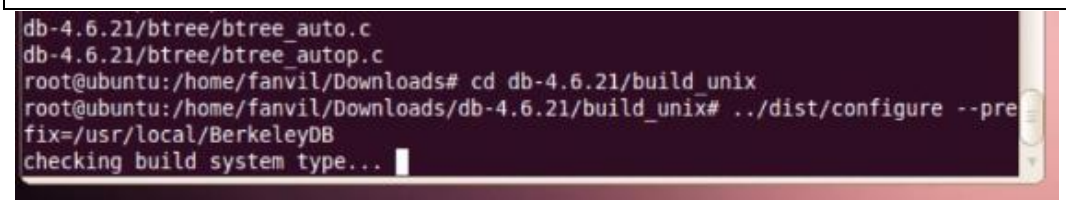

图 4-2-7

配置完成后如图 4-2-8

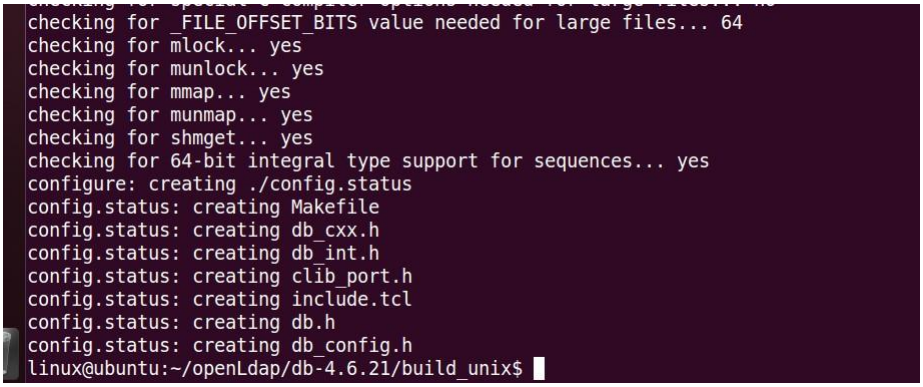

图 4-2-8

输入 make

```
#make
```

出现如图 4-2-9 提示表示没有问题，输入 make install

图 4-2-9

```
#make install
```

出现如图 4-2-10。BerkeleyDB 安装成功。

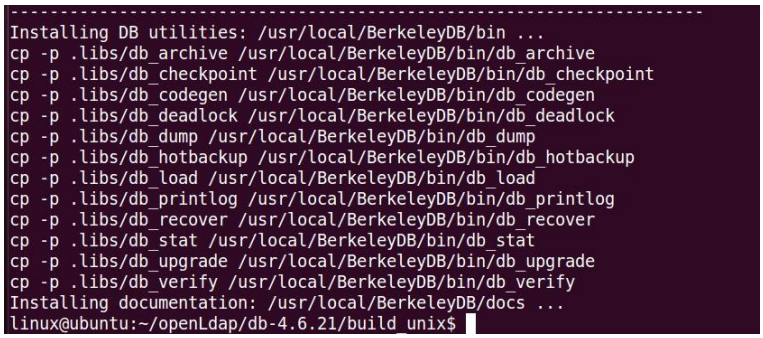

图 4-2-10

这时我们不要忘了配置库文件的搜索路径。输入如下命令

```
#echo "/usr/local/BerkeleyDB/lib" >> /etc/ld.so.conf
#ldconfig -v
```

4.2.3 安装 openldap

下载 openldap。这里我们选择的 openldap 版本是 2.4.40。输入解压命令

```
#tar xzvf openldap-2.4.40.tgz
#cd openldap-2.4.40
```

为了防止 openldap 和 BerkeleyDB 不兼容导致安装失败，先执行命令：

```
#exprot LD_LIBRARY_PATH="usr/local/BerkeleyDB/lib"
# export LD_LIBRARY_PATH="xxx/db-4.6.21/build_unix/.libs/"
Xxx 代表 db 的解压路径
```

之后配置环境

```
# env CPPFLAGS="-I/usr/local/BerkeleyDB/include" LDFLAGS="-L/usr/local/BerkeleyDB/lib" ./configure --prefix=/usr/local/openldap --enable-ldbm
```

这里如果碰到之前提出的不兼容问题，会有如图 4-2-11 的提示

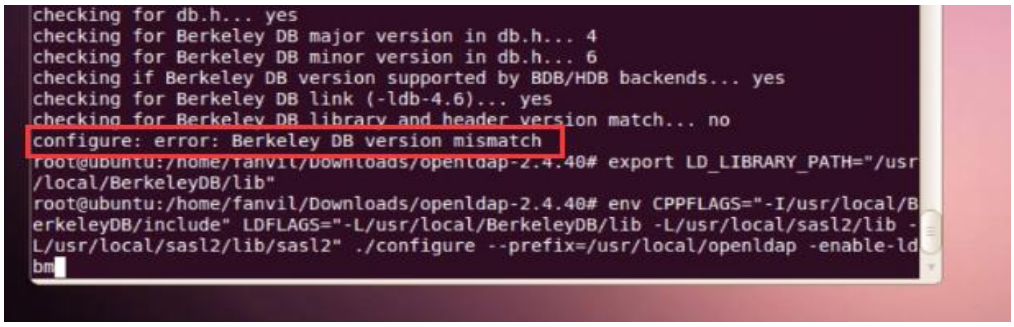

图 4-2-11

这里如果碰到下面的错误提示：

```
configure: error: BDB/HDB: BerkeleyDB not available
```

解决方法如下：

```
#export CPPFLAGS="-I/usr/local/BerkeleyDB/include"
#export LDFLAGS="-L/usr/local/BerkeleyDB/lib"
```

在出现图 4-2.12 的提示的 make depend 提示后，输入 make depend 指令

```
#make depend
```

图 4-2-12

在出现如图 4-2-13 的提示后输入 make 指令进行编辑

```
#make
```

图 4-2-13

出现如图 4-2-14 的提示后，编译成功，我们可以输入 make test 进行自测，该测试不是必需，但是可以帮助我们发现问题。该过程时间很长。

图 4-2-14

```
#make test
```

如果 make test 没有报错,我们就可以输入 make install 进行安装。如图 4-2-15

图 4-2-15

```
#make install
```

没有报错的话，服务器搭建完成。

4.3 配置

OpenLDAP 的主配置文件是：
/usr/local/openldap/etc/openldap/slapd.conf，需要注意的是，每次修改配置文件的设置后，都要重新起动 OpenLDAP 服务，这样才能使配置生效
这样，openLdap 在 linux 下安装完成，可以像上文中介绍的创建 test.ldif 导入条目。

```
# cd /usr/local/openldap/etc/openldap
```

编辑时需要根据自身的系统选择编辑工具，如果是图形化界面的可用 gedit

```
# gedit slapd.conf
```

找到该条语句

```
include /usr/local/openldap/etc/openldap/schema/core.schema
```

在该语句后添加以下语句

```
include /usr/local/openldap/etc/openldap/schema/corba.schema
include /usr/local/openldap/etc/openldap/schema/cosine.schema
include /usr/local/openldap/etc/openldap/schema/dyngroup.schema
include /usr/local/openldap/etc/openldap/schema/inetorgperson.schema
include /usr/local/openldap/etc/openldap/schema/java.schema
include /usr/local/openldap/etc/openldap/schema/misc.schema
include /usr/local/openldap/etc/openldap/schema/nis.schema
include /usr/local/openldap/etc/openldap/schema/openldap.schema
```

效果如图 4-3-1 所示

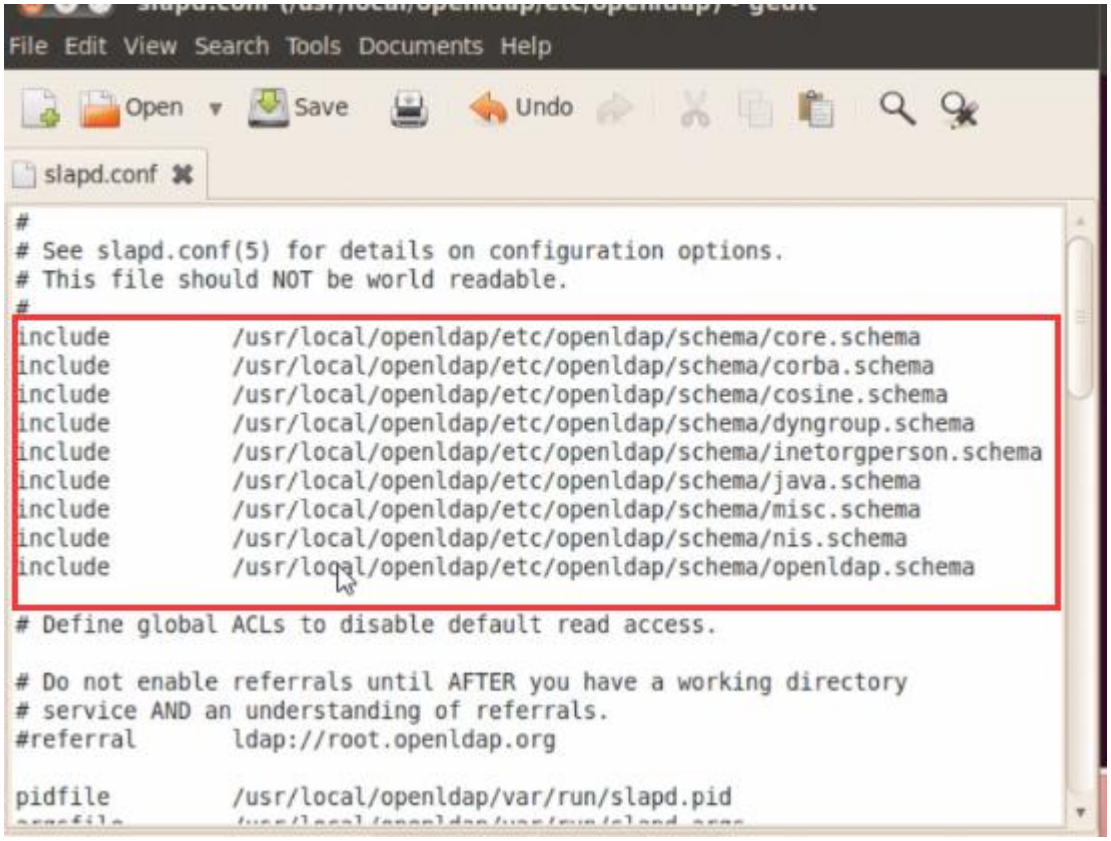

图 4-3-1

设置目录树：

suffix "dc=my-domain,dc=com"

改为：

suffix "dc=winline,dc=com"

<*注 1：这里可以自定义配置 dc=xxx,dc=com，对应话机设置中的“查询 base”>

设置管理员的 DN：

rootdn "cn=Manager,dc=my-domain,dc=com"

改为：

rootdn "cn=admin,dc= winline,dc=com"

<*注 1：这里可以自定义配置：cn=xxx,dc=xxx,dc=com，后半部分要与 suffix 相同>

设置管理员口令：

rootpw secret

改为：

root pw {SSHA}e7BBqjes5EF1grsupjvUfNkNdmZD+F6u

该结果是明文“miracle”经 SSHA 加密运算后的结果，有以下方法获得：

miracle@miracle-desktop:~$ sudo /usr/local/openldap/sbin/slappasswd

[sudo] password for miracle:

New password:

（输入你的密码）
Re-enter new password:
（再次输入密码）
然后就会生成加密后的密钥：{SSHA}e7BBqjes5EF1grsupjvUfNkNdmZD+F6u
{SSHA}wZ4AzwiU850mH1F95KwvBh+Dv2S21Dtn
<*注 1：管理员 DN 和管理员口令就是访问 LDAP 的用户名密码>
启动服务器输入下面指令：

```
#/usr/local/openldap/libexec/slapd
```

LDAP 的联系人是以文本形式导入，文本是 ldif 格式的 UTF-8 纯文本文件，导入命令：
/usr/local/openldap/bin/ldapadd -x -D "cn=admin,dc=miracle,dc=com" -W -f test.ldif

<*注 1：test.ldif 为要导入的文件，该命令在 test.ldif 文件夹下>
在搭建好 openldap 后首次需要导入根节点，

首次导入的文件格式：

```
dn: dc=winline,dc=com
dc: winline
objectclass: top
objectclass: domain
```

<*注 1：用于定义根节点 dc=winline,dc=com，接下来再添加的目录和联系人都将在这个根节点基础上添加>
导入成功后再次编辑文件，可根据实际情况添加目录或联系人。

```
dn: ou=fanvilShenZhen,dc=winline,dc=com
objectclass: organizationalUnit
ou: fanvilShenZhen

dn: ou=fanvilBeijing,dc=winline,dc=com
objectclass: organizationalUnit
ou: fanvilBeijing

dn: uid=use1,ou= fanvilBeijing, dc=winline,dc=com
objectClass: inetOrgPerson
objectClass: uidObject
cn: user1
sn: user1
telephoneNumber: 112123
mobile: 1234
```

再次导入该文件。

<*注 1：在重复编辑同一个文件时，导入一次的内容在下一次要删除，否则会有错误提示>

4.4 图形化管理工具

前面我都是手动编辑 ldif 文件来增加用户

针对 OpenLDAP 图形界面管理，开源组织也提供了 GUI 管理 OpenLDAP 软件，目前开源的产品有 phpLDAPadmin、LDAP Account Manager、Apache Directory Studio、LDAP Admin 等管理工具。如果有兴趣的话可以查看参考资料 3 进行详细了解，这里我们用之前介绍的图形化管理工具即可对 linux 下搭建的 ldap 进行管理。

5 如何在 Fanvil 话机上使用 LDAP 电话本

5.1 概述

LDAP 电话本支持以下功能：

- 最多可以配置 4 个 LDAP 电话本。
- 支持访问整个目录。
- 在拨打和接听时查找对方号码并把姓名更新到屏幕上。
- 支持自定义电话本的属性字段，包括姓名，电话本，移动电话和其他电话。
- 支持多种认证方式，包括无认证，简单认证，CRAM-Digest 认证和 CRAM-Digest 认证。

5.2 配置介绍

LDAP Settings	
LDAP	
描述	在配置中体现为 LDAP1 至 LDAP4。现在最多支持 4 个 LDAP 电话本，配置不同的 LDAP 电话本就是通过该配置进行切换。
Display Title	
参数	LDAPN Title :
描述	当前 LDAP 的标题名，显示在话机屏幕上
Version	
参数	LDAPN Version :
描述	配置区间：2 或 3 指明 LDAP 服务器的版本，默认版本是 3.
Server Address	
参数	LDAPN Server :
描述	指明 LDAP 的域名或 IP 地址
Server Port	
参数	LDAPN port :
描述	指明 LDAP 的端口，默认为 389
LDAP TLS Mode	
参数	LDAPN Use SSL :
描述	配置区间：0 ,1, 2 0：LDAP ：默认配置 与 LDAP 服务器进行不加密的连接 1：LDAPS ：与 LDAP 服务器之间建立 TLS/SSL 连接（默认 636 端口）

	2：LDAP TLS Start ：与 LDAP 服务器之间建立 TLS/SSL 连接（默认 389 端口）
Authentication	
参数	LDAPN Authenticate :
描述	配置区间 0,1,2,3 0：None 1：DIGEST - MD5 2：CRAM-MD5 3：Simple 默认配置
Calling Line	
参数	LDAPN Calling Line :
描述	AUTO: -1 Sip Line 1 至 6 : 1 至 6 指定拨打线路。当该指定线路呼出时，在与之匹配线路的 LDAP 电话本中查找联系人的信息。如果没有找到，在其他配置为 AUTO 的 LDAP 电话本中查找联系人信息。
Search Line	
参数	LDAPN Bind Line :
描述	AUTO: -1 Sip Line 1 至 6 : 1 至 6 指定接听线路。当该指定线路来电时，在与之匹配线路的 LDAP 电话本中查找联系人的信息。如果没有找到，在其他配置为 AUTO 的 LDAP 电话本中查找联系人信息。
Username	
参数	LDAPN Username :
描述	管理员用户名(当认证方式为 NONE，此处可不填)
Password	
参数	LDAPN Password :
描述	密码（当认证方式为 NONE，此处可不填）
Search Base	
参数	LDAPN Base :
描述	配置服务器要开始搜索的起始位置。
Max Hits	
参数	LDAPN Max Hits :
描述	最大采样数
Telephone	

参数	LDAPN Tel Attr :
描述	通过配置的属性来搜索 telephone number
Mobile	
参数	LDAPN Mobile Attr :
描述	通过配置的属性来搜索 mobile number
Other	
参数	LDAPN Other Attr :
描述	通过配置的属性来搜索 Other。
Name Attr	
参数	LDAPN Name Attr :
描述	通过配置的属性来搜索 Name（可以配置多个属性）
Sort Attr	
参数	LDAPN Sort Attr :
描述	查询到的结果以何种方式排序
Display name	
参数	LDAPN Displayname :
描述	通过配置的属性来显示姓名
Name Filter	
参数	LDAPN Name Filter :
描述	搜索姓名类属性时的范围 例如：配置为(|(cn=%)(sn=%))，且在搜索时输入字母 a： 意思为搜索所有以 a 开头的 CN 或 所有以 a 开头的 SN 属性。 例如：配置为(&(cn=%)(sn=%))，且在搜索时输入字母 a： 意思为搜索所有以 a 开头的 CN 且 以 a 开头的 SN 属性。
Number Filter	
参数	LDAPN Number Filter :
描述	搜索号码类属性时的范围 例如：(|(telephoneNumber=%)(mobile=%)(other=%))，且在搜索时输入数字 1： 意思为搜索所有以 1 开头的 telephoneNumber 或 所有以 1 开头的 mobile 或所有以 1 开头的 other 属性。 例如：(&(telephoneNumber=%)(mobile=%)(other=%)),且在搜索时输入数字 1： 意思为搜索以 1 开头的 telephoneNumber 且 以 1 开头的 mobile 且 以 1 开头的 other 属性。
Enable In Call Search	
参数	LDAPN In Call Search :
描述	配置区间：0 或 1

	0：关闭呼入查询 1：开启呼入查询
Enable Out Call Search	
参数	LDAPN Out Call Search :
描述	配置区间：0 或 1 0：关闭呼出查询 1：开启呼出查询

配置实例如图 5-2-1：

图 5-2-1

配置好以上查询条件并提交之后，便可在话机菜单 - 话簿 — LDAP 下从 LDAP 服务器下载符合查询条件的数据信息，下载后的通讯录信息可显示在话机中，用户可以根据需要进行直接呼叫、发送信息、查询联系人、加入本地电话簿、加入黑名单等操作。

5.3 LDAP 在话机上的使用

在网页端配置好后选择 menu - phoneBook - LDAP，进入下图所示的界面：如图 5-3-1 的 ldap1 为网页端配置的显示标题。

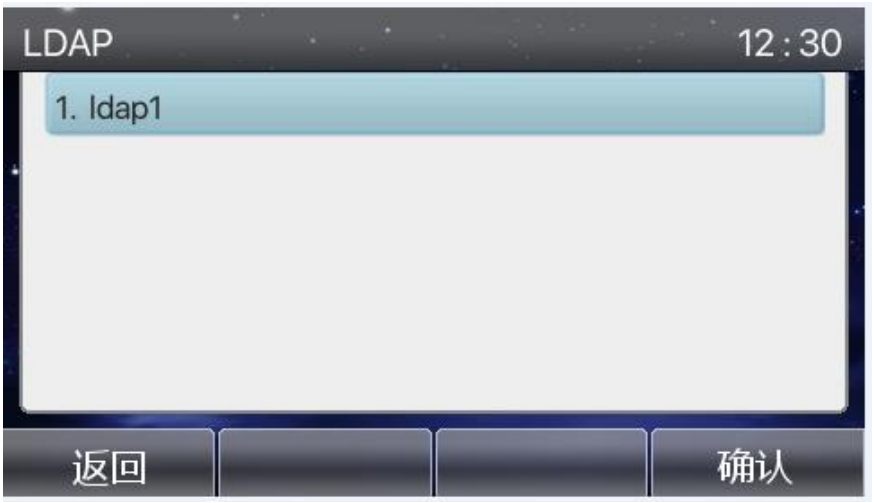

图 5-3-1

如图 5-3-2 这里的 fanvil 与查询 base 配置相关。

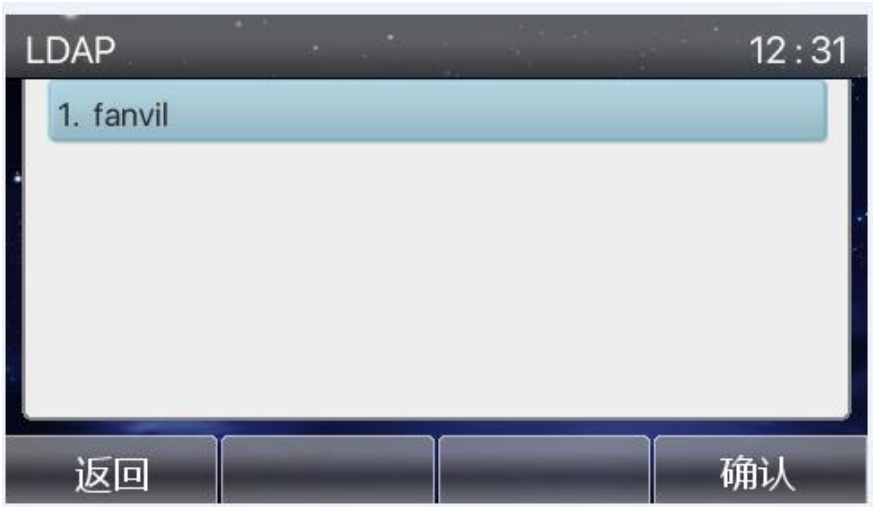

图 5-3-2

在点击确认后，我们可以看到 LDAP 电话本中的联系人信息，这里显示的联系人信息取决于配置的 name attr。这时我们可以通过”拨出”按钮拨打通话，如果联系人信息中同时存在办公号码或手机号码，会出现弹框提示选择拨出哪个号码。如图 5-3-3

图 5-3-3

选择一个联系人，选择：”配置”。即可看到联系人的详细信息，这里的办公号码的信息取决于配置的办公电话，手机号码的信息取决于配置的手机号码。如图 5-3-4

图 5-3-4